

ADDRESSING AMERICA'S DATA PRIVACY SHORT-  
FALLS: HOW A NATIONAL STANDARD FILLS  
GAPS TO PROTECT AMERICANS' PERSONAL  
INFORMATION

---

HEARING

BEFORE THE

SUBCOMMITTEE ON INNOVATION, DATA, AND  
COMMERCE

OF THE

COMMITTEE ON ENERGY AND  
COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

APRIL 27, 2023

**Serial No. 118-29**



Published for the use of the Committee on Energy and Commerce  
[govinfo.gov/committee/house-energy](https://govinfo.gov/committee/house-energy)  
[energycommerce.house.gov](https://energycommerce.house.gov)

U.S. GOVERNMENT PUBLISHING OFFICE

55-613 PDF

WASHINGTON : 2024

## COMMITTEE ON ENERGY AND COMMERCE

CATHY McMORRIS RODGERS, Washington

*Chair*

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

---

### PROFESSIONAL STAFF

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



SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE

GUS M. BILIRAKIS, Florida

*Chairman*

LARRY BUCSHON, Indiana

TIM WALBERG, Michigan, *Vice Chair*

JEFF DUNCAN, South Carolina

NEAL P. DUNN, Florida

DEBBIE LESKO, Arizona

GREG PENCE, Indiana

KELLY ARMSTRONG, North Dakota

RICK W. ALLEN, Georgia

RUSS FULCHER, Idaho

DIANA HARSHBARGER, Tennessee

KAT CAMMACK, Florida

CATHY McMORRIS RODGERS, Washington

*(ex officio)*

JAN SCHAKOWSKY, Illinois

*Ranking Member*

KATHY CASTOR, Florida

DEBBIE DINGELL, Michigan

ROBIN L. KELLY, Illinois

LISA BLUNT ROCHESTER, Delaware

DARREN SOTO, Florida

LORI TRAHAN, Massachusetts

YVETTE D. CLARKE, New York

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

*officio)*



## C O N T E N T S

	Page
Hon. Gus M. Bilirakis, a Representative in Congress from the State of Florida, opening statement .....	1
Prepared statement .....	4
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement .....	6
Prepared statement .....	8
Hon. Cathy McMorris Rodgers, a Representative in Congress from the State of Washington, opening statement .....	10
Prepared statement .....	12
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement .....	15
Prepared statement .....	17

### WITNESSES

Morgan Reed, President, ACT—The App Association .....	19
Prepared statement .....	21
Answers to submitted questions .....	158
Donald Codling, Senior Advisor for Cybersecurity and Privacy, REGO Payment Architectures, Inc. ....	40
Prepared statement .....	42
Answers to submitted questions .....	162
Edward Britan, Vice President, Associate General Counsel, and Head of Global Privacy, Salesforce, Inc. ....	48
Prepared statement .....	50
Answers to submitted questions .....	164
Amelia Vance, Founder and President, Public Interest Privacy Center .....	62
Prepared statement .....	64
Answers to submitted questions <sup>1</sup> .....	

### SUBMITTED MATERIAL

<i>Inclusion of the following was approved by unanimous consent.</i>	
List of documents submitted for the record .....	117
Article of May 24, 2022, “Remote learning apps shared children’s data at a ‘dizzying scale,’” by Drew Harwell, Washington Post .....	118
Letter of April 26, 2023, from Brad Thaler, Vice President of Legislative Affairs, National Association of Federally-Insured Credit Unions, to Mr. Bilirakis and Ms. Schakowsky .....	123
Letter of April 26, 2023, from Ashkan Soltani, Executive Director, California Privacy Protection Agency, to Mr. Bilirakis and Ms. Schakowsky .....	127
Letter of April 27, 2023, from Privacy for America to Mrs. Rodgers, et al. ....	131
Letter of April 27, 2023, from 1Huddle, et al., to Mr. Pallone, et al. ....	134

<sup>1</sup>Ms. Vance’s reply to submitted questions for the record has been retained in committee files and is available at <https://docs.house.gov/meetings/IF/IF17/20230427/115819/HMTG-118-IF17-Wstate-VanceA-20230427-SD001.pdf>.

## VI

	Page
Report of the Information Technology and Innovation Foundation, “The Looming Cost of a Patchwork of State Privacy Laws,” January 2022 <sup>2</sup>	
Letter of April 27, 2023, from Jim Nussle, President and Chief Executive Officer, Credit Union National Association, to Mr. Bilirakis and Ms. Schakowsky .....	137
Letter of April 27, 2023, from Ed Mierzwinski, Senior Director, Federal Consumer Program, U.S. PIRG, to Mr. Bilirakis and Ms. Schakowsky .....	140
Statement to the House Committee on Financial Services by Edmund Mierzwinski, Senior Director, Federal Consumer Program, U.S. Public Interest Research Group, February 26, 2019 .....	141

---

<sup>2</sup>The report has been retained in committee files and is included in the Documents for the Record at <https://docs.house.gov/meetings/IF/IF17/20230427/115819/HMTG-118-IF17-20230427-SD035.pdf>.

## **ADDRESSING AMERICA'S DATA PRIVACY SHORTFALLS: HOW A NATIONAL STANDARD FILLS GAPS TO PROTECT AMERICANS' PER- SONAL INFORMATION**

---

**THURSDAY, APRIL 27, 2023**

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

The subcommittee met, pursuant to call, at 2:02 p.m. in the John D. Dingell Room 2123 Rayburn House Office Building, Hon. Gus Bilirakis (chairman of the subcommittee) presiding.

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

Also present: Representatives Obernolte.

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.

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

Again, good afternoon and welcome to the 36th hearing the U.S. Congress has held on privacy and data security over the last 5 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 Sector's Gramm-Leach-Bliley Act; and the Fair Credit Reporting Act; and the healthcare'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:]

**Opening Statement of Chair Gus Bilirakis  
As Prepared for Delivery  
Committee on Energy and Commerce  
Subcommittee on Innovation, Data, and Commerce  
Hearing entitled “Addressing America’s Data Privacy Shortfalls: How a  
National Standard Fills Gaps to Protect Americans’ Personal Information”  
April 27, 2023**

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’m 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..... why 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 Byte Dance, exploit access to data..... where the FTC’s lines of jurisdiction and authority are and how that interplays with a 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 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’ll discuss sectoral data privacy regimes — like the financial sector’s Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, the health sector’s Health Insurance Portability and Accountability Act (HIPAA), the education sector’s Family Educational Rights and Privacy Act (FERPA), and of course the Children Online Privacy Protection Act – COPPA – which this subcommittee knows 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 risk and uncertainty that businesses could better avoid if we had clear rules of the road. This only gets more complicated as fifty different states move towards their own data privacy laws, meaning an increasingly complicated and confusing landscape for consumers and for business. Having clear rules in place will protect Americans, particularly our kids, as well as fuel innovation in the American marketplace.

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’s 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 GLBA and COPPA by protecting all kids under 18.



Ms. Vance, with the Public Interest Privacy Center, is a recognized expert on 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.

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

Mr. Reed, with the App Association, will discuss how this 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.

In closing, I want to thank all the witnesses for coming today. I want to thank Chair Rodgers and Ranking Member Pallone for all the progress we've made so far and their continued commitment to get this done, as well as Ranking Member Schakowsky who has made this effort a true partnership. I look forward to working with all of you on providing protections for Americans and certainty for businesses.

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 5 minutes for an opening statement.

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

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 5 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 healthcare, 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 on Energy and Commerce**

**Opening Statement as Prepared for Delivery  
of**

**Subcommittee on Innovation, Data, and Commerce Ranking Member Jan Schakowsky**

***Hearing on “Addressing America’s Data Privacy Shortfalls: How a National Standard Fills  
Gaps to Protect Americans’ Personal Information.”***

**April 27, 2023**

A majority of Americans agree: consumers need comprehensive federal data privacy protections.

Existing sector specific federal privacy laws leave consumers vulnerable to invasions of their privacy.

HIPAA protects health information you share with your doctor or hospital, but not information collected by most mobile health applications.

Financial information you share with your bank has some protections, but not most payment data shared with retailers.

FERPA protects student data, but does not protect a child who attends a private school or when a child downloads and uses an educational app at home.

These laws leave large gaps in their protections.

Big Tech has stepped into those gaps to collect ever more personal and intimate data about us and our children.

Tech companies profit off of our habits, our finances, who we love, where we live, and our most sensitive health data.

Every time you browse the web or wear a smart watch, a tech company is tracking you.

They use this data to manipulate us, to addict us, and to keep us on their platforms so we can be fed more ads.

Or they sell the data to the highest bidder so that companies you’ve never heard of can build profiles of you.

Over the past few years, the DOJ charged three data brokers for knowingly selling lists of vulnerable Americans to criminal scammers.

These companies profited off defrauding elderly Americans and people with Alzheimer’s.

April 27, 2023

Page 2

Enough is enough.

We need protections for all Americans that put consumers back in control of their data.

Americans are tired of feeling helpless online.

It is time to pass comprehensive federal data privacy legislation that protects consumers and fills the gaps in these sectoral laws.

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 5 minutes for an opening statement.

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

Mrs. RODGERS. 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 healthcare 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 na-

tional 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 cyberbullies, 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 Mrs. Rodgers follows:]

**Opening Statement of Chair Cathy McMorris Rodgers  
As Prepared for Delivery  
Committee on Energy and Commerce  
Subcommittee on Innovation, Data, and Commerce  
Hearing entitled “Addressing America’s Data Privacy Shortfalls: How a  
National Standard Fills Gaps to Protect Americans’ Personal Information”  
April 27, 2023**

Good afternoon and welcome.

This is our sixth privacy and data security hearing this year.

It will give 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 a near unanimous 53-2 vote...

...and included many safeguards to ensure activities in these various sectors remained 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 also they’re using our data to manipulate what we see and what we think.

This is especially true for our 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 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 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 cyberbullies, sexual predators, drug dealers, and others trying to do them harm.

This can't be allowed to continue.

I can't emphasize 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 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 their 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 we get this legislation right.

Our efforts have shown us that the single best way we can protect Americans in today's digital ecosystem is with a national data privacy and security standard.

And the American people agree.

More than 80 percent of Americans say they are looking for Congress to act.

It is our responsibility to ensure their data privacy and security, to provide even higher levels of protections for their kids, and to rein in Big Tech.

I look forward to the testimony and I yield back.

Mrs. RODGERS. 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 5 minutes for an opening statement.

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

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 and 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 healthcare 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. Sixty-four percent of children between 8 and 12 years old report watching online videos on platforms like TikTok and YouTube every day. Nearly one in five 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 popups 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 overcollection 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 on Energy and Commerce****Opening Statement as Prepared for Delivery  
of  
Ranking Member Frank Pallone, Jr.*****Innovation, Data, and Commerce Subcommittee Hearing on “Addressing America’s Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans’ Personal Information.”*****April 27, 2023**

For decades, we’ve 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’re 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’s 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. The iPhone wasn’t released until 2007. In internet years, these laws are dinosaurs.

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 does not apply to EdTech downloaded and used at home or in after school programs to supplement or complement children’s schoolwork.

April 27, 2023  
Page 2

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.

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. Sixty-four percent of children between eight- and twelve-years-old report watching online videos on platforms like TikTok and YouTube every day. Nearly one in five say they use social media every day.

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

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, gymnastics classes, or a broad variety of other activities, they share data about their children. 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.

That’s why we must pass a comprehensive privacy bill that closes the gaps and enshrines Americans’ right to privacy in law. We need a bill that reins-in the overcollection of information by mandating data minimization. We need a bill that puts all Americans back in control of how their data is collected, used, and shared.

Last Congress, this Committee overwhelmingly passed such a bill with broad bipartisan support. I’m committed to getting a bill over the finish line and look forward to continuing to work with Chair Rodgers on that effort.

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 5 minutes.

**STATEMENTS OF MORGAN REED, PRESIDENT, ACT-THE APP ASSOCIATION; DONALD CODLING, SENIOR ADVISOR FOR CYBERSECURITY AND PRIVACY, REGO PAYMENT ARCHITECTURES, INC.; EDWARD BRITAN, VICE PRESIDENT, ASSOCIATE GENERAL COUNSEL, AND 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—Thinkamigo 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 healthcare 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 nonstarter. 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 healthcare 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' character was stranded on a remote island in the movie *Cast Away*, 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:]





## Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information

---

*Testimony of*

Morgan Reed  
President  
ACT | The App Association

*Before the*

U.S. House of Representatives  
Committee on Energy and Commerce  
Subcommittee on Innovation, Data, and Commerce



1401 K Street NW  
Suite 501

202.331.2130  
[www.ACTonline.org](http://www.ACTonline.org)

@ACTonline  
[/ACTonline.org](https://www.facebook.com/ACTonline.org)

## I. Introduction

We applaud this Subcommittee for holding today's hearing to examine the privacy risks—and the vast benefits—of activities involving the collection and processing of consumer data adjacent to the sector-specific federal privacy frameworks. Small businesses in the app economy lead the way in solving problems and protecting privacy in these areas.

ACT | The App Association is a global trade group for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. Today, the App Association represents an ecosystem valued at approximately \$1.8 trillion and supports 6 million American jobs. Our members propel the data-driven evolution of these industries and compete against larger firms in a variety of ways, including on privacy and security protections.

Policymakers are appropriately curious and concerned about the privacy and security implications of data collection and processing around the edges of the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA), and Family Educational Rights and Privacy Act (FERPA). Given that the United States lacks an overarching, comprehensive privacy framework, the gaps between what consumers see as “health,” “finance,” and “education” are real. At the same time, this Subcommittee has also acknowledged that digital health, financial technologies (FinTech), and digital education tools provide expanded access to higher quality, more cost-effective services across these critical industries. The activity taking place in the penumbras around these silos is some of the most dynamic and beneficial economic activity the world has to offer, but the privacy and security sensitivities are also accordingly higher. They are the best reason for Congress to enhance federal privacy protections.

The layered applicability of the Federal Trade Commission (FTC) Act, FERPA, and HIPAA to real-life economic activity is deceptively complex. A comprehensive, risk-based privacy framework—like the American Data Privacy and Protection Act (ADPPA, H.R. 8152, 117th)—is the best option before Congress to clarify these complications, better protect consumers in and between the penumbras around federal privacy silos, and advance American digital economy competitiveness on the global stage.

We recommend Congress take the following into consideration as the Subcommittee continues its legislative work on comprehensive privacy legislation:

1. Simply “expanding” HIPAA is a non-starter.
  - HIPAA is an interoperability regime, designed for an incredibly narrow set of “covered entities” providing healthcare services to patients. Expanding that list to all entities processing data with any connection to health—like grocery stores—would

turn the Department of Health and Human Services (HHS) and its sub-agency, the Office of Civil Rights (OCR), into a second FTC, but one with a staff of 72 already overseeing 6,000 annual complaints and convert much of the economy into an interoperable system required to maintain data for audit purposes.

2. Financial services go beyond GLBA and need a risk-based framework to better empower consumers.

- Like HIPAA, GLBA applies to a narrow, already-defined group of entities. But unlike HIPAA, GLBA currently lacks consumer data access requirements. The outcome is that the GLBA silo sometimes traps financial information, making it more difficult for consumers to understand and control their information. A risk-based framework can make it clear to the industry what can be done and spur innovation.

3. FERPA overlaps with the FTC Act and its child privacy requirements, resulting in uncertainty for parents, commercial industries, and educational institutions alike.

- Instead of augmenting the risks these overlaps present by imposing age verification requirements or increasing data collection with a “constructive knowledge” threshold, a federal privacy law should modernize verifiable parental consent (VPC) requirements currently in place.

## II. Health Insurance Portability and Accountability Act (HIPAA)

*HIPAA Background.* HIPAA and its concomitant Privacy Rule is one of the most misquoted or at least most misinterpreted laws on the books. Contrary to popular punditry, HIPAA is an interoperability regime, designed to help insurers, providers, and patients have access to electronic health records and support interoperability. Of course, Congress understood that enabling easier portability would create privacy concerns, but the “how” and “why” was left open so that Congress might pass a more comprehensive privacy law to deal with the issues. Specifically, when HIPAA first passed, it did not specify the kinds of privacy or security requirements the OCR should impose. Instead, the HIPAA statute included a “shot clock” provision implicitly authorizing what eventually became the Privacy Rule and the Security Rule, if Congress failed to authorize them directly within three years after HIPAA’s initial enactment (by August of 1999).<sup>1</sup> That provision required OCR to send a report to Congress in 1997 with recommendations on how legislation governing health information privacy should look. Preemptively addressing future legislative gridlock, the statute further provided that, “If legislation governing standards with respect to the privacy

<sup>1</sup> Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, Sec. 264, available at <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>.

of individually identifiable health information . . . is not enacted by the date that is 36 months after the date of enactment of this Act, the Secretary . . . shall promulgate final regulations containing such standards.”<sup>2</sup> OCR finalized the Privacy Rule and Security Rule in 2003.

Congress should not defer entirely to agency rules like this again.

*Scope and summary of HIPAA.* HIPAA applies to two classes of entity: covered entities (CEs) and their business associates (BAs). Similar to the General Data Protection Regulation’s (GDPR’s) classification of “controllers” and “processors,” HIPAA directly applies to the “controller” analogue, CEs (health plans, providers that process insurance claims electronically, and clearing houses). This aspect of HIPAA’s scope is notable. Most consumers would be surprised to know that the main touchstone for HIPAA’s applicability to their health services is whether the provider processes insurance claims electronically. The “processors” in HIPAA parlance are BAs, which are only BAs to the extent they provide services on behalf of CEs but are liable for compliance with HIPAA via their contracts with CEs. Finally, HIPAA’s provisions apply to CEs’ and BAs’ activities with respect to protected health information (PHI), which includes personally identifiable information (PII) that is created or received by a healthcare provider, among other entities; relates to past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; and that either identifies the individual or “with respect to which there is a reasonable basis to believe the information can be used to identify the individual.”<sup>3</sup> The Privacy Rule generally allows CEs to use or disclose PHI for the purposes of “treatment, payment, and other routine healthcare operations.”<sup>4</sup> With some caveats, the Privacy Rule only allows any other use or disclosure of PHI if the CE obtains the patient’s written “authorization.”<sup>5</sup> Several administrative requirements also apply to CEs, including a requirement to provide individuals with written notices summarizing the Privacy Rule’s provisions and patients’ rights, along with contact information for someone at the CE who can handle privacy complaints and other communications. The Privacy Rule also requires CEs to designate a privacy official to develop and implement its policies and procedures and mandates disclosure—and therefore retention—of PHI for purposes of an OCR audit or investigation. Finally, CEs must obtain written assurance from BAs that they would use PHI only for the purposes permitted or required by contract, and “implement appropriate safeguards to prevent misuse of PHI.”<sup>6</sup>

*The app economy is revolutionizing digital health.* Several App Association members serve patients via BA agreements with CEs. That puts their core activities under the scope of

---

<sup>2</sup> *Id.*, at Sec. 264(c)(1).

<sup>3</sup> 45 C.F.R. Sec. 160.103.

<sup>4</sup> 45 C.F.R. Sec. 164.506.

<sup>5</sup> 45 C.F.R. Sec. 164.508.

<sup>6</sup> CONG. RESEARCH SERV., HIPAA PRIVACY, SECURITY, ENFORCEMENT, AND BREACH NOTIFICATION STANDARDS 6 (updated Apr. 17, 2015), available at <https://crsreports.congress.gov/product/pdf/R/R43991>.

HIPAA. For example, Rimidi provides a remote physiologic monitoring and clinical decision support platform for patients and their caregivers to manage a variety of chronic conditions. Similarly, Podometrics provides a thermometric foot mat enabling caregivers to monitor patients at risk of developing diabetic foot ulcers (DFUs), identifying DFU development up to five weeks before they present clinically and preventing limb amputation. As digital health companies augmenting the caregiving services of healthcare providers, these member companies' activities are subject to HIPAA via BA agreements. Our member companies' digital health tools are only becoming more important for patients, consumers, and caregivers. With the current physician shortage of about 30,000 expected to increase to up to 124,000 by 2034;<sup>7</sup> healthcare costs spiking;<sup>8</sup> the efficacy of sensors and software that collect and analyze physiologic health data improving dramatically;<sup>9</sup> and the pandemic forcing patients to rely more generally on virtual care services, digital health tools are now an important fixture in American healthcare that can augment caregivers' reach and capabilities while controlling costs.

Some of our member companies provide services for clients and customers other than CEs subject to HIPAA, but nonetheless process sensitive PII with some connection to health. For example, App Association member Particle Health allows patients to receive and share their medical information digitally, seamlessly, and affordably. Importantly, Particle Health empowers consumers to make use of their health records both inside of the HIPAA umbrella and outside its borders. Particle Health's role in the digital health ecosystem is simple: Particle is the "Plaid of digital health."<sup>10</sup> If that comparison doesn't ring any bells, Plaid is the company that provides Venmo and other third-party financial services applications the programming interface to securely connect and transfer funds from a consumer's bank account to that specific payment app. Particle wants to serve the same function for digital health records, so that consumers have an easier, privacy-maximizing way to transfer their information from medical institutions to the various applications, platforms, and services they desire. Another company outside the scope of HIPAA, WeStrive, provides personal fitness trainers several digital tools to create programming for clients and monitor their progress. Consumers and trainers should be able to put sensitive health data to work with apps like WeStrive's, knowing that the law provides optimal privacy and security protections. WeStrive should not be thought of as failing to protect PII because bad actors in this space are culpable of privacy abuses,

<sup>7</sup> American Assoc. of Medical Colleges, "AAMC Report Reinforces Mounting Physician Shortage," press release (Jun. 11, 2021), available at <https://www.aamc.org/news-insights/press-releases/aamc-report-reinforces-mounting-physician-shortage>.

<sup>8</sup> "Lowering Unaffordable Costs: Legislative Solutions to Increase Transparency and Competition in Health Care," Hearing before the House Committee on Energy and Commerce, Subcommittee on Health, 118th Cong. (Apr. 26, 2023), available at [https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/lyse%20Schuman\\_Witness%20Testimony\\_04.26.23.pdf](https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/lyse%20Schuman_Witness%20Testimony_04.26.23.pdf).

<sup>9</sup> Aisha Malik, "Garmin launches a new FDA-cleared ECG app for the Venu 2 plus," TECHCRUNCH (Jan. 24, 2023), available at <https://techcrunch.com/2023/01/24/garmin-new-fda-cleared-ecg-app-venu-2-plus/>.

<sup>10</sup> See Matt Schwartz, "2020 Vision: Will Congress Have Foresight on Healthcare Privacy?" ACT | THE APP ASSOCIATION BLOG (Jan. 21, 2020), available at <https://actonline.org/2020/01/21/2020-vision-will-congress-have-foresight-on-healthcare-privacy/>.

which reporting sometimes unfairly implies is the case with all digital offerings outside HIPAA. A federal privacy framework would better enable WeStrive to earn consumers' trust.

*Health privacy abhors a vacuum.* Congress' decision in HIPAA to essentially defer entirely to HHS to create a health privacy regime has imposed avoidable costs on patients and would likely impose even greater costs on consumers in the general privacy context. As we noted in a letter to this Committee in 2021,<sup>11</sup> one of the most important reasons for Congress to enact a general privacy law is to enhance patients' privacy and security protections with respect to sensitive PII, especially as they relate to digital health activities outside the HIPAA umbrella. Congress' failure to act poses three related risks on this point: 1) that health privacy abuses are more likely to continue, undermining legitimate digital health offerings and weakening consumer trust; 2) that the FTC will continue to experience pressure to adopt overly expansive interpretations of its authority; and 3) that states will continue to take increasingly divergent approaches to health privacy outside the scope of HIPAA.

Without specifically arming the FTC with the authority to enjoin privacy harms, evidence suggests adverse headlines will continue, although the Commission is making use of its current tools. The FTC's recent consent orders show that it has prioritized punishing privacy and security abuses by digital health companies that may run afoul of FTC Act prohibitions on unfair or deceptive acts or practices. The FTC sought to enjoin health services companies outside the scope of HIPAA from telling their customers that they were not sharing their PII but doing so anyways for advertising purposes. For example, in one complaint, the FTC alleges that a company, "recognizing the sensitivity of this health information, . . . repeatedly promised to keep it private and use it only for non-advertising purposes such as to facilitate consumers' therapy,"<sup>12</sup> but then shared some PII with third parties for advertising. In another case, the FTC alleged that a period tracking app told its users that no PII would be shared with third parties but used software development kits (SDKs) that shared their PII with several advertisers.<sup>13</sup> Advertising and marketing are critical to making digital health tools accessible for consumers and patients, but it is equally important that digital health providers adhere to privacy representations as well as customer expectations.

At the same time, the FTC is also seeking to expand its current tools absent a new privacy law that would enhance penalties and clarify its authority specific to privacy and security. For example, although privacy experts have always distinguished between purposeful disclosures and data breaches, the FTC recently interpreted its Health Breach Notification

<sup>11</sup> Letter from Morgan Reed, president, ACT | The App Association, to Hon. Frank Pallone, chairman, House Committee on Energy and Commerce, and Hon. Cathy McMorris Rodgers, Republican leader, House Committee on Energy and Commerce, Re: Fed. Trade Comm'n Settlement with Flo (Feb. 17, 2021).

<sup>12</sup> Fed. Trade Comm'n, *BetterHelp, Inc.*, FTC No. 202316, Complaint (released Mar. 2, 2023), available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/2023169-betterhelp-complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/2023169-betterhelp-complaint.pdf).

<sup>13</sup> Fed. Trade Comm'n, *Flo Health, Inc.*, FTC No. 1923133, Complaint (released Jan. 13, 2021), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc>.



Rule (HBNR) as a privacy rule. As then-Commissioner Wilson noted in a dissent, the statement expansively and awkwardly interprets a few aspects of the rule, including the definition of vendors of “personal health records” (PHRs), to which the rule applies.<sup>14</sup> She argued further that interpretations of a rule that differ in such a way from the text of its provisions typically require an administrative rulemaking procedure so that an agency can consider comments from the public. More fundamentally, the core of the HBNR is a requirement to notify affected consumers in case of a “breach of security,” defined as “acquisition of [PHR identifiable health information] without the authorization of the individual.”<sup>15</sup> There are two problems with applying this rule when a company purposely transfers data to a third party. First, such transfer is generally done under color of authorization by the affected consumer—in other words, the company has (erroneously but deliberately) inferred the consumer’s authorization for its transfer. Characterizing the willful transfer by a company to a third party as a “breach of security”—which typically involves a malicious attack by a third party that thwarts the company’s security measures—is at least an odd fit. The second problem with the interpretation is that it merely requires notice to the consumer for purposely transferring the data, instead of punishing the act of transferring the data. Going forward, a company could potentially comply with the broadly interpreted HBNR by simply notifying consumers after the fact that it has given their health information to Facebook. It could still be liable under Section 5 of the FTC Act as well, and that is the proper *current* law to apply in this scenario. But better than either option would be a privacy law that empowers the Commission to pursue and punish instances of purposeful onward transfer of health PII that is inconsistent with a company’s own representations, the context of its relationship with the affected consumers, or data minimization requirements.

For a few years, states have steadily adopted new comprehensive privacy laws that differ in various ways from each other. However, in the wake of the Supreme Court of the United States’ (SCOTUS’) decision in the *Dobbs v. Jackson Women’s Health Org.*, the gap between state approaches to privacy is widening at an accelerated pace. For example, Washington recently enacted a new consumer health privacy law, the Washington My Health My Data Act,<sup>16</sup> and a few other legislatures like Connecticut’s and Maryland’s are considering similar measures. Despite that legislators mainly sought to protect consumers against investigations into access to reproductive health services that are legal in Washington, the law does not address law enforcers’ access to reproductive health data. Instead, it broadly proscribes collection, processing, or transfer by commercial actors of an exceptionally broad class of information that may relate to an individual’s health. As noted above, even HIPAA allows for the collection, transfer, and processing of PHI for treatment, payment, and other routine operations. The My Health My Data Act prohibits any collection

---

<sup>14</sup> Fed. Trade Comm’n, Policy Stmt. On Breaches by Health Apps and Other Connected Devices, Dissenting Stmt. Of Comm’r Christine S. Wilson, FTC No. P205405 (Sept. 15, 2021), *available at* [https://www.ftc.gov/system/files/documents/public\\_statements/1596356/wilson\\_health\\_apps\\_policy\\_statement\\_dissent\\_combined\\_final.pdf](https://www.ftc.gov/system/files/documents/public_statements/1596356/wilson_health_apps_policy_statement_dissent_combined_final.pdf).

<sup>15</sup> 16 C.F.R. Sec. 318.2(a), 318.3(a).

<sup>16</sup> My Health My Data Act, Wash. House, HB 1155, 68th Leg. (2023).

or transfer of consumer health data, with only two exceptions: 1) with consent of the consumer for “a specified purpose” and 2) to the extent *necessary* to provide a product or service the consumer has requested.<sup>17</sup> The prohibitions in this law appear to restrict WeStrive from improving its product to benefit consumers, or create a new data-driven feature that helps trainers and consumers reach their fitness or health goals. We agree with policymakers that the law should not allow app developers to create profiles on people using their sensitive PII in ways that contravene the context of the relationship they have with consumers or fail to gain their consent. However, only allowing two narrow bases for collection and transfer of consumer health data—including non-health information which can be used to extrapolate health-related information—would limit consumers’ access to digital health tools. The answer to privacy and security risks involving consumer health data should not be to drastically limit consumers’ ability to make use of them and incidentally sweep in non-health digital services in the process. The approach in ADPPA strikes a more reasonable balance that would punish privacy and security harms arising from collection and processing of health information—and impose reasonable data minimization requirements that mitigate unnecessary risks associated with the creation and maintenance of profiles—while allowing for product improvements, context-driven communications, and basic operations.

*Information blocking rules.* As part of the 21st Century Cures Act, Congress required HHS (via its National Coordinator for Health IT Policy or ONC) to prohibit entities subject to HIPAA from blocking a patient’s access to their own protected health information (PHI). The information blocking rules add further pressure on Congress to regulate privacy outside the scope of HIPAA because if they work as intended, they should empower patients to transfer their own PHI outside the HIPAA umbrella. CEs and BAs that collect and process PHI on behalf of patients worry about their own liability for transferring PHI to entities not subject to HIPAA, even at their patients’ request. Entities subject to HIPAA tend to lack a detailed understanding of—and underestimate—the FTC’s and state attorney generals’ (AGs’) enforcement practices regarding health privacy, but their concerns are not unjustified. Despite our Connected Health Initiative’s (CHI’s) suggestion for ONC to require privacy and security attestations by health apps receiving PHI on behalf of patients under the information blocking rules, ONC declined to adopt such a requirement. Requiring health apps and device companies to make those attestations would have equipped consumer protection enforcers with statements that could be matched against the companies’ own conduct, setting up deception claims against companies behaving inconsistently with their representations. But ultimately, attestations would be a stopgap measure until Congress can enact a risk-based general privacy law that would prevent and penalize collection and processing activities involving health information that impose costs in excess of their benefits.

*HIPAA is a bad fit for digital health tools provided directly to consumers.* For example, some of the most important aspects of a general privacy bill are the requirements to respond to various kinds of consumer requests. One such requirement mandates that

---

<sup>17</sup> *Id.*, Sec. 5.



covered companies respond to verified consumer requests to delete PII pertaining to them. Although this protection should be limited by legitimate business or legal interests associated with maintaining PII, it is an important one in the general economy. However, the policy interest in allowing patients to request their healthcare providers to delete health information about them is generally weaker, while the policy interest in blocking such requests is stronger. A patient may want to delete addiction information about themselves in their health records, but that information may save their lives in the future. Thus, a central aspect of a strong consumer privacy regime probably should not even be a feature of patient privacy as applied to HIPAA CEs and BAs. Specific provisions aside, a regime like HIPAA designed around the patient-provider relationship is not well suited to consumer products. The main purpose of HIPAA is to ensure interoperability between health providers so that a patient can port their health records across providers. Thus, HIPAA is supposed to be a bulwark against the incentive for providers to block access by the patient in order to keep the patient's business, as well as the disincentive to invest anything in making health records accessible or readable by other providers. Consumer-facing products and services with health-related aspects are fundamentally different and appropriately require an approach more along the lines of what this Subcommittee is pursuing taking a risk-based approach to privacy and security protections. For this reason, we strongly support updated language in ADPPA that would clarify that PHI is exempt from ADPPA's requirements.

To the extent Congress wants to intervene to ensure interoperability between digital health services outside of HIPAA, we would recommend cosponsoring and forwarding the Better Interoperability for Devices (BID) Act (H.R. 1557). The BID Act would require the Food and Drug Administration to make recommendations to Congress as to how it could better allow for interoperability between medical devices inside and outside the HIPAA umbrella.

*Federal consumer privacy law must enable healthcare research and necessary processing activities on behalf of consumers.* Comprehensive privacy bills like ADPPA will likely include data minimization provisions. One aspect of the HIPAA framework that is appropriate for digital health tools outside of HIPAA is an allowance for those services to conduct health research and process payments and other healthcare functions on behalf of customers. To the extent federal legislation imposes data minimization restrictions on covered companies, they should appropriately allow for the use of covered data for research, especially "peer-reviewed scientific, historical, or statistical research," that "adheres to all relevant laws" governing such research, as ADPPA provides.<sup>18</sup> It is essential for a comprehensive federal privacy bill not to inadvertently hamstring legitimate medical research that currently benefits consumers and patients.

---

<sup>18</sup> American Data Privacy and Protection Act, Sec. 1(b)(10) (H.R. 8152, 117th Cong.).

### III. Gramm-Leach-Bliley Act (GLBA)

*GLBA Scope.* GLBA applies to “financial institutions,” which the regulation defines as entities engaged in any activity that is “financial in nature,” or is “incidental to such financial activities as described” in the Bank Holding Company Act.<sup>19</sup> The FTC is the primary data security regulator of financial institutions under GLBA, which imposes security requirements, disclosure limits, and transparency requirements. GLBA authorizes two separate rulemakings, the Safeguards Rule (vested solely in the FTC) and the Privacy Rule (which four separate federal agencies maintain and enforce, divided up by entity type).<sup>20</sup> GLBA distinguishes between “consumers” and “customers” of financial institutions. Consumers are individuals who interact with a financial institution, while customers are consumers who have an ongoing relationship with the financial institution.<sup>21</sup> For example, a person who applies for a loan from a financial institution—and therefore submits sensitive, non-public PII—is a consumer; but they only become a customer if they have an ongoing relationship with the financial institution.

*The FinTech app economy.* The app economy activity in and around the scope of GLBA is robust. Our FinTech member companies are solving emerging and long-intractable problems for consumers. For example, Goalsetter provides a financial education platform for children, which allows kids to receive allowance or monetary gifts from friends, parents, and relatives, and/or spend money through the Goalsetter debit card. Another kids’ digital wallet company, REGO, has gone so far as to patent the COPPA compliant opt-in protections in its Mazoola mobile wallet for kids.<sup>22</sup> Both of these FinTech apps put parents in charge and empower kids to learn financial literacy. With studies indicating that just over half of Americans are considered financially literate and only 24 percent of millennials understand basic financial concepts,<sup>23</sup> App Association members and companies like them are leveraging the power of smart devices and platforms to address this issue in privacy-protective ways.

Just as patients sought a remedy for better access to their records through the information blocking rules, concerns about customers’ access to and portability of their financial information have punctuated financial services policy debates. The App Association filed comments on the Consumer Financial Protection Bureau’s (CFPB’s) statutorily required

<sup>19</sup> 16 C.F.R. Sec. 314(b); Sec. 314(h)(1).

<sup>20</sup> 16 C.F.R. Sec. 314; 16 C.F.R. Sec. 313.

<sup>21</sup> 16 C.F.R. Sec. 314.2(b); Sec. 314.2(c).

<sup>22</sup> See MAZoola: A KIDS MOBILE WALLET POWERED BY PRIVACY, available at <https://mazoola.co/>.

<sup>23</sup> Kevin P. Chavous, “A Hand Up Or A Handout? Tackling America’s Financial Literacy Crisis,” FORBES (Feb. 3, 2022), available at <https://www.forbes.com/sites/stopaward/2022/02/03/a-hand-up-or-a-handout-can-we-tackle-americas-financial-literacy-crisis/?sh=2258745fe251>.

Section 1033 rulemaking<sup>24</sup> highlighting the need for more meaningful access by customers to their own financial information. As we noted in our letter, “[t]he opportunities for consumers in the open market are enormous. FinTech applications can improve consumer access to credit using data points that traditional lenders overlook; they can allow consumers to budget and receive personalized tips in real time; and they can send consumers sophisticated analytics tailored specifically to them and their goals.”<sup>25</sup>

Unfortunately, “the current data access regime involves a mixture of informal credentials-based access agreements and formalized, token-based access agreements. This system is complicated to navigate for both consumers and third parties and often allows traditional financial institutions to impose their will regardless of consumer welfare.”<sup>26</sup> These unnecessary levels of friction resulted in some FinTech companies playing fast and loose with consumer expectations, opting to “scrape” data from their banking screens in order to populate their apps.<sup>27</sup> Even though this was typically done to effectuate what the developers assumed was their customers’ intent, it never involved actual notification to the consumer and consent, because it was done outside the managed lines of communication and contract. Just as the information blocking rules require electronic health records (EHR) companies to adopt open application programming interfaces (APIs), we also recommended that financial institutions enable safe, secure access—with appropriate data security and privacy guardrails—by customers to their own financial data via open APIs. Having established the overwhelming policy interests in enabling consumers to access their own financial information and transfer it outside the GLBA umbrella, an equally important task is to ensure consumers continue to benefit from optimal privacy and security protections outside the scope of GLBA. The answer must be a federal, risk-based privacy framework.

## IV. Family Educational Rights and Privacy Act (FERPA)

<sup>24</sup> Letter from Morgan Reed, president, ACT | The App Ass’n, to Hon. Rohit Chopra, Dir., Consumer Financial Protection Bureau, Re: Comments of ACT The App Association on the Consumer Financial Protection Bureau’s *Request for Information Regarding Consumer Access to Financial Records*, Docket No. CFPB-2016-0048, 81 Fed. Reg. 83806 (Feb. 21, 2023).

<sup>25</sup> *Id.* (citing AITE-NOVARICA, *ALTERNATIVE DATA ACROSS THE LOAN LIFE CYCLE: HOW FINTECH AND OTHER LENDERS USE IT AND WHY*, (2018), available at [https://www.experian.com/assets/consumerinformation/reports/Experian\\_Aite\\_AltDataReport\\_Final\\_120418.pdf?elqTrackId=7714eff9f5204e7ca8517e8966438157&elqaid=3910&elqat=2](https://www.experian.com/assets/consumerinformation/reports/Experian_Aite_AltDataReport_Final_120418.pdf?elqTrackId=7714eff9f5204e7ca8517e8966438157&elqaid=3910&elqat=2); PwC, *GLOBAL FINTECH REPORT 2019: CROSSING THE LINES - HOW FINTECH IS PROPELLING FS AND TMT FIRMS OUT OF THEIR LANES*, (2019), available at <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2019.pdf>.)

<sup>26</sup> *Id.*

<sup>27</sup> Benjamin Pimentel, “Banks and fintechs agree: It’s time for screen scraping to go. So what’s next?” *PROTOCOL* (Oct. 5, 2021), available at <https://www.protocol.com/fintech/idx-financial-data>.

*Scope of FERPA.* FERPA's scope is not as narrow as it seems, and the gap it leaves is made smaller by the FTC's proactive approach. Similar to HIPAA and GLBA, FERPA also applies primarily to a specific class of entity—educational agencies and institutions—and a subset of personal information, “education records.” The definition of education records, in turn, is tied to whether educational agencies or institutions are directing the processing or collection<sup>28</sup> and includes any information “directly related to a student.” The two pillars of FERPA are 1) a requirement for schools allow parents access and review of their children's education records; and 2) a prohibition on schools from releasing students' education records without written consent of their parents, unless one of several exceptions apply.<sup>29</sup> Notably, FERPA's requirement to allow students' parents to access education records distinguishes it to some extent from other federal privacy silos and from state laws that apply adjacent to the federal laws. Observing shortcomings in the access requirements in GLBA and HIPAA, policymakers have sought to perfect the requirements in those contexts in ways that have not materialized as clearly under FERPA.

Notably, just as the HIPAA Privacy Rule refers to contractual entities working on behalf of CEs as BAs, the U.S. Department of Education's (ED's) rules promulgated under FERPA also create categories analogous to “business associate.” The statutory provisions Congress enacted do not explicitly contemplate third-party companies providing digital education services using education records. However, schools routinely release education records to third-party education services companies—without incurring the requirement to obtain parental consent for disclosure—via the statutory exception allowing schools to provide such records to “school officials.” ED's regulations spell out the relationship more concretely. To qualify for the school officials exception, schools must determine whether a third party “(1) performs an institutional service or function for which the agency or institution would otherwise use employees; (2) is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) is subject to the requirements of Sec. 99.22(a) governing use and redisclosure of personally identifiable information from education records.”<sup>30</sup>

*The app economy is thriving in education technology.* Thinkamigo is an educational app company focused on getting kids excited about writing. Their app, Story Dice, helps give kids ideas for stories, while their apps Lists for Writers and Story Spark help kids lay out their story, build out their characters and plot points, and give them the tools they need to improve their overall writing and story structure. Through contracts with school districts, Thinkamigo provides these tools for students in the school context, which puts their activities under the scope of FERPA. But to the extent that the apps are available to kids and parents directly, COPPA and the FTC Act are the federal laws covering their privacy practices. Another member company, TORSH, provides a platform for teachers'

<sup>28</sup> 20 U.S.C. Sec. 1232g(a)(4)(A). Education records are materials that “contain information directly related to a student” and “are maintained by an educational agency or institution or by a person acting for such agency or institution.”

<sup>29</sup> 20 U.S.C. Sec. 1232g(a)(1)(A); 20 U.S.C. Sec. 1232g(b)(1).

<sup>30</sup> 34 C.F.R. Sec. 99.31(a)(1)(i)(B).

professional development, enabling streamlined review, analysis, and management of classroom video clips.<sup>31</sup> The ability for schools to rely on digital tools like TORSH's is critical and increasingly important as we exit the pandemic.

*COPPA applies to entities subject to FERPA.* It is difficult to address FERPA requirements without also covering the FTC Act and one of its subsections, COPPA, which regulates collection of PII about children under 13. There is no explicit carve-out from the FTC Act or COPPA for entities subject to FERPA. In fact, the FTC is adamant that COPPA applies readily to education technology companies, even when they are subject to FERPA via contractual relationships with schools.<sup>32</sup> However, COPPA rules do attempt to account for potential conflicts or incongruities between the two regimes. For example, COPPA's requirement for companies to obtain verifiable parental consent (VPC) prior to collecting PII from children does not apply "to the extent permitted under other provisions of law," (presumably, including FERPA's provisions).<sup>33</sup> This could lead to the two regimes applying slightly unevenly or confusingly, even though there might be good reasons for their overlapping structure, but the FTC has addressed the issue. Under FERPA, schools need not obtain parental consent for disclosing children's education records to educational apps on contract with the school. The FTC has clarified in a frequently asked questions (FAQ) section that an education technology company may rely on "consent obtained from the school under COPPA instead of the parent,"<sup>34</sup> when such collection is for the "use and benefit of the school and for no other commercial purpose."<sup>35</sup> Conversely, if the same children (if they are 12 or younger) sought to use the same educational apps outside the school context, the app must obtain VPC directly from those children's parents.<sup>36</sup> Thus, while the edges around sector-specific privacy laws may seem less regulated, in this case, more regulatory privacy barriers arguably exist under the FTC framework than under the sector-specific law.

The FTC's COPPA guidance for education technology companies emphasizes that students should not have to trade access to digital education services for their privacy.<sup>37</sup> This messaging addresses rapidly developing privacy concerns over the past three years, especially among parents, as the COVID-19 pandemic caused schools to move to a virtual model leaning heavily on digital tools. Parents worried that their children's mandatory use

<sup>31</sup> TORSH, POWER PACKED FEATURES DRIVE RESULTS, available at <https://www.torsh.co/features/>.

<sup>32</sup> Fed. Trade Comm'n, Policy Stmt. of the Fed. Trade Comm'n on Education Tech. and the Children's Online Privacy Protection Act (May 19, 2022), available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf) (FTC EdTech Policy Statement).

<sup>33</sup> 16 C.F.R. Sec. 312.5(c)(6)(iv).

<sup>34</sup> Fed. Trade Comm'n, Complying with COPPA: Frequently Asked Questions, N. COPPA AND SCHOOLS, Question N.1, (Jul. 2020), available at <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS>.

<sup>35</sup> *Id.*, at N.2.

<sup>36</sup> 15 U.S.C. Sec. 6501(9); Sec. 6502(b)(1)(A)(ii); 16 C.F.R. Sec. 312.5.

<sup>37</sup> FTC EdTech Policy Statement at 4, "Children should not have to needlessly hand over their data and forfeit their privacy in order to do their schoolwork or participate in remote learning, especially given the wide and increasing adoption of ed tech tools."

of those services would expose their children to undue privacy and data security risks, in an environment where no in-person alternative was available. Against this backdrop, the FTC sought to remind consumers and parents that the FTC Act—including COPPA—still applies to education technology companies. Most notably, the FTC reminded education technology companies that COPPA's prohibitions on 1) conditioning access to a service on a child disclosing more information than is reasonably necessary for the child to participate in an activity; 2) engaging in commercial activities like marketing, advertising, or other commercial activities unrelated to the provision of the school-requested service; 3) retaining PII about a child longer than reasonably necessary to fulfill the reason for which it was collected; and 4) failing to have procedures to maintain the confidentiality, security, and integrity of children's PII, *still apply* to education technology companies, even when they also comply with FERPA.

The FTC's and ED's separate jurisdiction over different kinds of entities help illustrate how they fit together. The FTC has jurisdiction over commercial entities—not schools—while ED has jurisdiction over schools receiving federal education funds. Thus, ED's enforcement mechanism is limited to punishing schools—not education technology companies directly—by withholding their federal education funds. Similarly, the FTC Act does not authorize the FTC to enjoin schools from activities that result in consumer harm related to privacy and security. Where ED's jurisdictional limits suggest a gap in protections may exist, the FTC's guidance and policy statements make a strong case that federal privacy enforcers are holding education technology companies and schools accountable for privacy and security practices. Nonetheless, we have two suggestions as you consider updates to the FTC Act when it comes to children's and students' privacy:

1. Any amendments to or expansion of COPPA's protections to cover children up to 17 years old **should also modernize VPC requirements**. We have written extensively about the issues VPC present by shifting the onus for privacy protections to parents and consumers rather than companies providing services.<sup>38</sup> Expecting parents to provide credit card information, driver's license scans, or to call a 1-800 number to verify their identity for each online service with which their children interact is asking a great deal of today's parents. As the FTC itself has alluded to, parents now have little choice but to enable their children to make beneficial use of digital services. Requiring multiple redundant copies of their PII to exist in all corners of the internet their children may need to venture becomes a less workable concept with each passing day.
2. Any general consumer privacy legislation addressing kids' **privacy should avoid imposing age verification requirements or requirements that would require similar levels of data collection** to “verify” or “assure” a child's identity for age verification

---

<sup>38</sup> Letter from Morgan Reed, president, ACT | The App Association, to Hon. Maria Cantwell, chair, Senate Committee on Commerce, Science, and Transportation, and Hon. Ted Cruz, ranking member, Senate Committee on Commerce, Science, and Transportation, Re: Feedback/suggestions for improvement regarding the Kids Online Safety Act (KOSA) (S. 3663, 117th), available at <https://actonline.org/wp-content/uploads/2023-03-01-ACT-KOSA-letter-Senate-Commerce-and-Sponsors-FINAL.pdf>.

purposes. Similar to the issue described above, requiring detailed PII profiles on children to exist in multiple parts of the ecosystem with every company providing services a child may access introduces more serious privacy and security risks than are necessary. In fact, such requirements may conflict with other privacy provisions of a federal bill, especially those that apply to more sensitive classes of information like biometric indicators.<sup>39</sup> We also discussed this in testimony last year in the context of a privacy bill possibly moving COPPA to a “constructive knowledge” regime, which would require covered companies to compile much more granular profiles on children.<sup>40</sup>

## V. Conclusion

Each of the federal privacy silos that exist today present unique challenges for this Subcommittee to consider as you continue to work on a comprehensive privacy bill. Although COPPA applies to entities covered by FERPA, and the FTC Act overlays HIPAA, the sector-specific laws apply more narrowly than is often appreciated, causing gaps to appear wider than they are. As is often the case, the truth about activity around the federal privacy silos is both less shocking and more interesting than it appears at first glance. These market activities happen to be some of the most important areas for consumers and job creation in the United States and are therefore worth preserving and strengthening with a federal data privacy and security law. We look forward to continuing to work with this Subcommittee on federal privacy reform in the 118th Congress.

---

<sup>39</sup> Eric Goldman, “Do Mandatory Age Verification Laws Conflict with Biometric Privacy Laws? – Kuklinski v. Binance,” TECH. AND MARKETING L. BLOG, Apr. 8, 2023, *available at* <https://blog.ericgoldman.org/archives/2023/04/do-mandatory-age-verification-laws-conflict-with-biometric-privacy-laws-kuklinski-v-binance.htm> (“The invasiveness of [age verification] requirements could overwhelm and functionally moot most other efforts to protect consumer privacy.”).

<sup>40</sup> “Protecting America’s Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security,” Hearing before the House of Representatives Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce (comments of Graham Dufault, sr. dir. for public policy, ACT | The App Association).



## Appendix:

# The App Economy in Your District

### Majority

#### Chair: Bilirakis, FL-12

Since 2011, Tampa-based Thinkamigo is a husband-and-wife team working together to build family-friendly, education-focused mobile apps. Their apps range from interactive dice meant to take young writers to inspired storytellers to imagination-driven spy kits complete with virtual disguises, including a voice changer!

#### Vice Chair: Walberg, MI-05

Located in Jackson, Lean Rocket Lab is a coworking space and accelerator supporting businesses of all types by providing office space, education, mentorship, and pathways to funding for companies in a variety of industries. Their Manutech Incubator program and i4.0 Accelerators focus on startups creating devices and the software that powers them in manufacturing, transportation, data analytics, healthcare, and more.

#### Bucshon, IN-08

Located in Evansville and founded in 2016, anu is working to help people grow their own food through technology in order to create a more sustainable world and allow people to increase their food independence. With 11 employees, anu is building hydroponic farming systems that can grow anything from lettuce and other vegetables to any number of fruits or spices.

#### Duncan, SC-03

Topography Digital is a full-service software development company that focuses on providing services for small and medium-sized companies across industries looking to build or grow their digital presence or offerings. Their services include web and app development, drone programming, and cloud optimization.

#### Dunn, FL-02

TechFarms, founded in 2015 and located in Panama City Beach, has a singular mission: create a more technology-focused and vibrant entrepreneurial ecosystem in northwestern Florida. The team at TechFarms has created a collaborative coworking space for local business owners with the goal of lifting up the whole community.

#### Lesko, AZ-08

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



**Pence, IN-06**

Located in Muncie and founded in 1987, Accutech provides software solutions and services to those in the financial industry. Accutech's solutions include a wealth management platform, mobile applications that make opening an account easy, as well as a business intelligence dashboard.

**Armstrong, ND-At Large**

North Dakota-based Bushel built a digital ecosystem that powers APIs, apps, websites, and digital payment solutions to support agribusinesses and build digital infrastructure for the agriculture industry. Supporting more than 2,000 grain facilities with 40% grain origination in the United States and Canada, the Bushel platform strengthens relationships between grain processing facilities and farmers by enabling both to complete transactions quickly, safeguard important data, share information faster, and create a more complete picture of businesses.

**Allen, GA-12**

Zapata Technology is a veteran-owned Augusta-based cybersecurity company that provides critical cyber-secure infrastructure for the defense industry. Their products, offered globally, support persons in active duty with cybersecurity penetration testing, cloud computing and analytics, systems engineering and data integration, and custom software development.

**Fulcher, ID-01**

Located in Coeur d'Alene, Chief Architect Software provides automated residential home design and interior decorating software for architects, builders, and designers. Through their suite of software products, industry professionals can create construction drawings and floor plans, get 3D renderings of interior spaces and elevations, and 360-degree panoramic renderings of whole buildings to better understand and craft design schemes unique to each building project.

**Harshbarger, TN-01**

Located in Kingsport, Code & Color is a digital marketing firm that offers software and design services and helps businesses grow through creative design. Their main services are clustered into marketing, design, websites, and mobile apps.

**Cammack, FL-03**

Founded in 2001, Atmosphere Apps is based in Gainesville and is a custom software development shop that works with clients through the design, development, maintenance, and integrations with other popular technologies. Atmosphere Apps also maintains their client's apps long after development ensuring the apps are always up to date with OS versions and compliance standards. While initially focused on clients in the health sector, Atmosphere is expanding its client base to include sales, media, and travel industries.

**McMorris Rodgers, WA-05**

Founded in 2017, Gestalt is a 31-person team working to bring healthcare into the 21<sup>st</sup> century by replacing microscopes and glass slides with automated, electronic, and digital workflows. They provide services related to pathology in the medical field to professionals as well as those in education or academic research from their HQ in Spokane

**Minority:****Ranking Member: Schakowsky, IL-09**

The one-woman team at Kidz Learn Applications has been developing iOS and Android mobile apps that provide educational content to children for the past decade. Kidz Learn Applications has developed over 20 apps with lessons ranging from math to vocabulary and even created a guide for educational, kid-friendly places in New York City for a day of fun for kids and adults alike.

**Castor, FL-14**

Located in Tampa nearly 200 employees, Accusoft, originally founded as Pegasus Imaging Corporation in 1991, focuses primarily on content processing through image and document cleanup while providing APIs and barcode collection through mobile apps. They also provide digital conversion tools that turn paper document and paper-based processes (often found in legal, financial, and health transactions) into customized digital processes based on each client's unique needs.

**Dingell, MI-06**

Founded in 2017 and headquartered in Kalamazoo, with two other offices in the state, SPARK Business Works is a custom software development and design firm. They help businesses of any size create an effective online presence that aims to improve each client's unique needs for the connected customer experience.

**Kelly, IL-02**

Based in Kankakee and founded in 2020, Pathfinder is a full-service creative marketing agency that helps their clients tell stories through web and mobile solutions. With 24 currently employed, their offerings include web development, graphic design, photography, and other digital marketing offerings.

**Blunt Rochester, DE**

Located in Wilmington, MightyCall is a cloud-based communications and customer service platform founded in 2013. Their virtual phone system is designed specifically for small businesses and remote teams making it easy for teams to connect from anywhere through mobile and desktop apps. Their apps provide unique features like call availability windows, scheduling services, and the ability to mask personal cell numbers, given that privacy is a core pillar of MightyCall's service.

**Soto, FL-09**

Originally founded as "Yelling Across Cubicles"—because it was essentially built as a digital walkie-talkie to be used in the workplace—Yac was founded in 2019 in Kissimmee. Since then, Yac has grown to include other functionalities including asynchronous meetings, voice messages, screen sharing and shareable links, all focused on making remote work more collaborative.

**Trahan, MA-03**

Founded in 1997 and located in Maynard, Fisheye Software focuses on building enterprise-level software that makes complex systems easier to understand. They provide services to a number of clients, both in the government and commercial systems, contributing to anything from data archiving to air traffic control or missile defense systems.

**Clarke, NY-09**

Since Stellar Health's founding in 2018, this Manhattan-based healthcare technology company has rapidly grown to over 200 employees and is providing connected health solutions to patients everywhere. Stellar Health helps deliver providers targeted recommendations to enable "value-based" improvements to care and financial performance to hospitals. This means that through Stellar Health's services, patients receive care faster and at a lower cost throughout the care chain.

**Pallone, NJ-06**

DealerApp Vantage, located in Piscataway, is the nation's leading native mobile app development company that specializes in automotive dealers. They have mobile app solutions aimed to fit all budgets and sizes, from small, single rooftop dealerships to some of the largest auto groups in the United States.

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 5 minutes.

#### STATEMENT OF DONALD CODLING

Mr. CODLING. Commerce Committee Chair McRodgers, 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 cybersecurity operations. These programs particularly emphasize cybersecurity challenges that impact the global financial services, energy, and healthcare 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 preteens 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 nonaffiliate 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 nonaffiliated 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:]

**U.S. House of Representatives Committee on Energy & Commerce****Subcommittee on Innovation, Data, and Commerce****Hearing on Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information"****Prepared Testimony of Donald Codling, Rego Architectures, Inc. Senior Advisor for Cybersecurity & Privacy**

April 27, 2023

Commerce Committee Chair McMorris Rodgers, Ranking Member Pallone, Subcommittee Chair Bilirakis, Ranking Member Schakowsky, and Members of the Subcommittee.

Thank you for inviting me to testify. My name is Donald Codling, and I am a Senior Advisor to Rego Payment Architectures, Inc. ("REGO") for Cybersecurity and Privacy. For over 23 years, I worked in the FBI in various investigative programs focusing on International Cyber Crime and Cyber National Security Operations. These programs particularly emphasized cybersecurity challenges that impact the global financial services, energy, and healthcare industries. I was the principal liaison officer to DHS US-CERT and ICS-CERT for the FBI and was the lead supervisor for the Cyberstorm II and III national cyber exercises. I also served as the FBI's chairman of an international cybercrime working group consisting of the heads of Cyber Investigative Departments in Australia, Canada, New Zealand, the United Kingdom, and the United States.

Currently, I work as a CISO or CPO advisor to various FinTech companies, such as REGO. Using my experience in cybercrime, I advise companies' employees and Executive Management staff to craft a comprehensive cybersecurity and data privacy digital platform, combining core cyber hygiene, cyber threat intelligence, social media, and data privacy compliance tools.

My experience in cybersecurity and the FBI have taught me to identify areas of cyber risk and assess its threat. What we are experiencing now 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% of children under the age of 8 have either a smartphone or tablet they use exclusively. This is up from 41% in 2011. Secondly, the COVID-19 pandemic doubled consumer adoption of cashless payments, [according to a report by Mastercard](#), citing 79% of survey respondents prefer contactless payments post-pandemic. Finally, the purchasing power of the under-18 demographic has significantly increased in recent years. According to a [report by the National Retail Federation](#), 87% of a family's purchases are influenced by their children. In the same report, pre-teens are reported to spend their own money at over twice the

volume as they did 10 years ago. Retailers, advertisers, and fintech companies know that the under-18 market is big business. However, what has not been in place is the legal framework to incentivize kids' privacy by design in the financial industry.

This “perfect storm” of financial and technology trends is exacerbated by the fact that 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 (COPPA) makes it unlawful for online companies to collect and share the personal information of children under 13 without a parent’s consent. This is an opt-in process, where the parent must actively agree to such data collection and sharing. However, most fintech companies that provide financial service products to children adhere to the privacy protections of the Gramm-Leach-Bliley Act of 1999 (GLBA). Under GLBA, companies must offer an opt-out option for **non-affiliate** data sharing, but there is no opt-out for **affiliate** sharing. This means the default setting for these websites and financial apps allows for collecting and sharing data of children 13-17 with non-affiliated third parties unless the parent proactively opts out. Of even greater concern, there is no ability for parents to opt out of the sharing of their child’s financial transactions between affiliated companies.

How much data is being collected? According to [a report by SuperAwesome](#), a London-based company that helps app developers navigate child-privacy laws, by the time a child reaches age 13, mobile apps have collected over 72 million data points from that one individual. What kind of data? Names, birth dates, email addresses, GPS location history, purchase history, likes, dislikes, behavioral profiles and more – all designed to deliver targeted ads – all without the parent’s consent.

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’m 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. Since its inception in 2008, REGO has invested millions of dollars to build the technological framework that not only protects and safeguards the data and privacy of kids, but a family digital wallet experience that cannot function without the explicit consent and approval of the parent. The core of REGO was built around the concept of data minimization, where the only information collected for children under 17 is date of birth, and only because the app stores of Google and Apple require it. Strict parental controls are applied to every aspect of the REGO experience, such as requiring parental approval for others to deposit money into their child’s account or restricting kids to purchase items from only parent-approved vendors – critical security features that popular mobile payment apps do not have but should.

REGO was primarily designed as a white label offering for banks and credit unions, giving them the ability to provide a secure family banking platform that is fully branded and integrated into the financial institution. Through partnerships with banking core and technology providers, banks and credit unions can now more easily offer parents useful financial literacy tools with the comfort of knowing their children’s data is not being collected or shared. Individual users can experience REGO by downloading Mazoola, an

award-winning family digital wallet app that was built on the certified COPPA and third-party GDPR compliant platform.

In my experience, no other financial technology platform has child data and privacy protection so integrated in its core offering than REGO. That is only the result of over a decade of development, and a deliberate strategy to offer the most secure product regardless of the regulatory environment.

For these reasons, I am pleased to see recent bipartisan efforts to improve our nation's stance on protecting the data privacy of Americans, including our children. During her opening statements at the House Committee on Energy and Commerce on April 19, 2023, Chair Cathy McMorris Rodgers stated, "The American Data Privacy and Protection Act included the strongest internet protections for children of any legislation last Congress."

Ranking Member Jan Schakowsky, in the same hearing, added, "Most Americans worry about their data privacy and are concerned it is not being protected. I wanted to call attention to the American Data Privacy and Protection Act in which we say that we would require all data brokers to register...and with one push of a button, you can take yourself out."

Representative Kathy Castor remarked that, "The U.S. has fallen too far behind in prioritizing the protection of all people online, but especially young people. Because we do not have a national data privacy standard, we are currently stuck with this patchwork of state laws and narrow protections that leave a wide swath of our neighbors vulnerable to privacy abuses, including by data brokers."

I testify today, on behalf of REGO, regarding the importance of Congress passing comprehensive federal privacy legislation that will include updating privacy laws to protect children of all ages and in all circumstances. We support legislation that provides greater transparency to how our data is being used and the ability to control how that data is shared. Most importantly, we support legislation that provides a legal incentive and framework for companies to incorporate the kind of critical data protection processes and technologies to safeguard our children's data, especially as more young Americans are becoming active in the consumer marketplace at an earlier age. It was the sole purpose of protecting children's financial data and privacy that led to the creation of REGO. We sincerely hope to serve as an example of what can and should be done. We urge other companies to join us in our commitment to preserve the future safety of America's children.

Thank you again for giving me the opportunity to participate today. I look forward to your questions.



REGO is the first and only **COPPA certified** and **GDPR compliant** e-commerce solution enabling the under-18 age group to **manage and spend** money within a **parent-controlled** environment.



Family digital wallet platform

# Capabilities of REGO



**BANKING**

*Checking, savings and investing*

Custodial Accounts on COPPA and GDPR Compliant Platform. Offers FI Custodial Accounts with Mobile Wallet across age groups



**RETAIL**

*In-store and ecommerce*

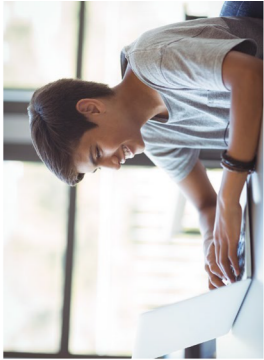
COPPA and GDPR compliant commerce buy flow and transactions (private). White Label Option for FI eCommerce integration for online child shopping.



**SOCIAL**

*Secure purchase platform*

Enables social platforms with COPPA and GDPR compliant finance transaction capabilities. Unlocks Gen-Z purchase potential with parent-control ecosystem.



**ANALYTICS**

*Compliant customer insights*

COPPA and GDPR Compliant data capture and persona views and insights. API access to COPPA and GDPR compliant datasets

# REGO was built with child privacy at its core



## COPPA

*Certified by PRIVO*

REGO is the first and only family wallet to be COPPA certified by [PRIVO](#), one of 6 organizations authorized by the FTC to provide the Safe Harbor seal

## GDPR

*Compliant by PRIVO*

REGO has also been determined by PRIVO to be compliant with GDPR, the world's leading standard of data privacy.

## PARENTS FIRST

*Secure Platform*

REGO empowers parents with financial literacy tools that manage where their children spend, save and give.

## SECURE TECH

*Patented Technology*

Through patented technology, only REGO provides unique tools for age verification, parental controls and wish list capabilities.

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

You are recognized, sir, for 5 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 2 years at Salesforce, 7 years at Microsoft, and 7 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 healthcare held—data held by providers and health plans. HIPAA fails, however, to cover health-related data that may be collected by noncovered 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:]

**Written Testimony of Edward Britan**

**Vice President, Associate General Counsel, and  
Head of the Salesforce Global Privacy Team**

**Salesforce, Inc.**

**Before the  
House Energy & Commerce Subcommittee on Innovation, Data, and Commerce**

**Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to  
Protect Americans' Personal Information**

**April 27, 2023**

## **I. Introduction**

**Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee,** thank you for providing me the opportunity to share my views on addressing gaps in U.S. privacy law through comprehensive federal privacy legislation. Comprehensive federal regulation of personal information is urgently needed to protect individuals, empower businesses, and advance responsible innovation.

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. I have spent almost two decades focused on helping companies comply with global privacy and data protection laws, including the past two years at Salesforce, the seven years before that at Microsoft, and the previous seven years helping a range of companies as a lawyer at Alston & Bird, LLP.

### **U.S. Leadership in Privacy**

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 2018.<sup>1</sup> 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 countries lacking a comprehensive national privacy law. The UK, Japan, Brazil, China, Kenya, and Thailand have all passed comprehensive privacy laws since GDPR went into effect.

---

<sup>1</sup> Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing 95/46/EC (General Data Protection Regulation).

This is disappointing because the U.S. had been a thought leader in this space. In fact, the core concepts in GDPR and most other global privacy laws build upon ideas introduced in a 1973 report published by the U.S. Department of Health, Education and Welfare (the “HEW Report”).<sup>2</sup> The HEW report introduced rights to access, delete and correct data, the data minimization and accuracy 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.<sup>3</sup> 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 50<sup>th</sup> 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.

I am honored to have this opportunity to share with you the importance of passing a comprehensive federal privacy law and the features and concerns that such a law should address.

## **II. Why We Need a Comprehensive Federal Privacy Law**

### **Salesforce Perspective**

Salesforce is a cloud computing company offering customer relationship management (CRM) and other business-focused software to businesses, governments, non-profits, and other

---

<sup>2</sup> U.S. Dep’t of Health, Education and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* viii (1973), <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>.

<sup>3</sup> Marc Benioff, Time for Silicon Valley to Get Behind a National Privacy Law, Politico (June 19, 2018), <https://www.politico.com/agenda/story/2018/06/19/silicon-valley-national-privacy-law-000679>.



organizations around the world. Our online and mobile services help our customers connect with their customers, being consumers, employees or citizens. Our customers use our services to work with some of their most sensitive data, which is why trust has been our number one value since our founding almost 25 years ago. A loss of that trust would jeopardize our ability to continue innovating and remain competitive. Therefore, Salesforce is committed to continuously proving to our customers that we are trustworthy custodians of their data.

To that end, we have developed a comprehensive privacy and data protection program that accounts for the ever-evolving landscape of global data protection laws. But we do not stop there. We also build our products using privacy by design principles and educate our customers regarding how they can use our products responsibly.

#### **Privacy Is a Fundamental Human Right**

Beyond the business imperative, Salesforce recognizes privacy as a fundamental human right that is crucial to upholding other rights, such as freedom of life, liberty, speech and protection against discrimination. To this end, we apply legal requirements that further the fundamental right to privacy, including from GDPR and other laws, globally. For us, protecting privacy is not merely a business strategy, but a moral responsibility. We urge Congress to help fulfill this responsibility by passing a comprehensive privacy law in the U.S. that applies to all Americans in all contexts.

#### **Americans Are Demanding Privacy Protection Louder Than Ever**

Americans want the government to hold companies accountable for how they process their personal information. This is borne out in a recent KPMG study in which 90% of

respondents indicate that government has a role to play in ensuring accountability.<sup>4</sup> Further, this belief does not seem to vary significantly according to political party, as a recent Pew Research Center study indicates that a majority of Americans – regardless of political affiliation – strongly favor increased legal protections governing companies’ use of their personal information.<sup>5</sup>

#### **A Broad Federal Privacy Law Should Support Existing Sectoral Laws**

The U.S. has not yet taken the same comprehensive approach to privacy as was recommended by the HEW report and effectuated with GDPR. Rather, privacy protection in the U.S. is sectoral and driven by issue-specific laws at the federal level. However, while U.S. law regulates privacy differently from the EU, these U.S. sectoral laws are also effective and influential. What is missing is comprehensive regulation of personal information that should support these sectoral laws.

Without such comprehensive rules there will be significant gaps in protection. For instance, the Health Insurance Portability and Accountability Act (HIPAA) protects data related to a physical or mental health condition, provision of health care, or payment, as processed by certain entities, including health care providers, health plans and health care clearinghouses. This excludes a vast amount of health-related data processed by non-covered entities, such as through connected devices and online services designed to monitor and improve health and fitness. A law carrying forward concepts from GDPR and recently-passed state laws would strictly regulate this data and the companies that process it.

---

<sup>4</sup> KPMG LLP, The new imperative for corporate data responsibility (2020), <https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf>.

<sup>5</sup> Pew Research Center, *Americans and Privacy: Concerned and Feeling Lack of Control Over Their Personal Information* (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

Similarly, while the Fair Credit Reporting Act (FCRA) effectively regulates consumer reporting agencies that furnish consumer reports, it does not cover similar types of profiling conducted by other companies for other purposes such as delivering personalized content or conducting e-commerce. Such profiles could be used in ways that impact an individual's reputation and privacy and should also be regulated.

Following passage of GDPR in 2018, the states have been filling this gap in U.S. privacy law by passing comprehensive laws of their own. California was the first state to take such action with the California Consumer Privacy Act of 2018 (CCPA). Since then, comprehensive privacy laws have also been passed in Virginia, Colorado, Connecticut, Montana, Utah, Iowa, Indiana, and Tennessee. While CCPA focused on restrictions around sharing personal information with third parties, the eight states that have subsequently passed laws, as well as a subsequent California law amending CCPA, the California Consumer Privacy Rights Act (CPRA), more closely adhere to the global standard set into motion by the HEW report and effectuated with GDPR.

Salesforce welcomes the passage of strong comprehensive privacy laws at the state level. These state-level efforts are important, as they demonstrate the need and demand for comprehensive privacy law. However, one's level of privacy should not depend on a ZIP code. Congress should be inspired to build upon these state-led efforts in setting a national standard which ensures that these privacy protections apply to all Americans.

### **III. What a Comprehensive Federal Privacy Law Should Address**

#### **Sensitive Data**

The broad regulation of personal information should include enhanced protections for specific types of sensitive data, such as data related to race, gender, ethnicity, religion, disability, and health-related data not governed by HIPAA. Such regulation would be directly beneficial for promoting equality and civil rights by forcing companies to proactively identify, evaluate, and counter potential discriminatory impacts.

#### **Emerging Technology – Mandatory Assessment**

Salesforce has publicly raised concerns that certain types of technology, like facial recognition, currently pose a high risk of harm and discriminatory impacts, particularly for underserved communities. Because of these concerns, we don't offer facial recognition capabilities in our products.<sup>6</sup> But we continue to engage with these emerging technologies and have established guidelines for the responsible and ethical development of generative AI, which we're committed to following as the technology continues to advance.<sup>7</sup>

We believe that thoughtful regulation can enable development of appropriate safeguards that allow companies to responsibly innovate and unlock the economic and growth opportunities for themselves and for all Americans. In particular, we believe there's substantial value in

---

<sup>6</sup> Salesforce, Why We've Never Offered Facial Recognition (June 15, 2020), <https://www.salesforce.com/news/stories/why-weve-never-offered-facial-recognition/>.

<sup>7</sup> Paula Goldman, Generative AI: 5 Guidelines for Responsible Development, Salesforce (February 7, 2023), <https://www.salesforce.com/news/stories/generative-ai-guidelines/>.

performing data impact assessments and/or algorithmic impact assessments, as proposed under the American Data Privacy and Protection Act (ADPPA), when there's a high potential or risk of harm. We know that data sets used to train AI models are often discriminatory, and that unfortunately, discriminatory training data will yield discriminatory model outputs. To counter this, U.S. law should mandate that companies undertake assessments to purposefully and proactively identify and analyze data sets and how they will be used as a means to counter any latent discrimination or bias that may exist in the data.

### **Core Privacy Principles and Civil Rights**

Salesforce strongly supports U.S. adoption of the core principles that underlie most global privacy laws, including GDPR. These principles, which were highlighted in the National Telecommunications and Information Administration's 2018 request for comments,<sup>8</sup> include transparency, control, data minimization, security, individual rights of access, correction, and deletion, risk management, and accountability.

Additionally, we believe that comprehensive federal privacy legislation should include provisions prohibiting the use of personal information to discriminate on the basis of protected characteristics. So we strongly supported inclusion in the ADPPA of "the first significant, nationwide expansion of civil rights protection in over a decade"<sup>9</sup> and would hope to see such protections included in future privacy legislation.

---

<sup>8</sup> Notice and Request for Comments, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018) ("RFC").

<sup>9</sup> Bertram Lee, Federal privacy legislation the protects civil rights is critical for all Americans, The Hill (July 21, 2022), <https://thehill.com/opinion/congress-blog/3568525-federal-privacy-legislation-that-protects-civil-rights-is-critical-for-all-americans/>.

**Controller/Processor Distinction**

It is a current best practice in global data protection laws and regulations to make important distinctions between companies that decide how and why to collect and process personal data, who act as controllers of that data, and companies that provide services and process data on behalf of controllers, who act as processors of the data.<sup>10</sup> These distinctions date back 40 years and have been enshrined in GDPR and other leading data protection laws and regulations around the globe.<sup>11</sup> They are also reflected in the ADPPA, which recognizes that companies have different responsibilities when operating in different capacities. When companies focus on their role in handling personal data about individuals, they can more effectively identify and implement controls to help protect the privacy of those individuals.

In most global data protection frameworks, controllers and processors each have equally important obligations to ensure consumers' privacy. Controllers determine the purpose and means for collecting and using data, so they have direct responsibilities to consumers. For example, controllers are expected to disclose how they will use the data they collect and how long they will retain the data, and promptly respond to consumer requests to access or delete their personal information. Processors provide services to controllers under legal and contractual obligations that require them to only handle data at the specific direction of the controller, protect the data with adequate security measures, and allow controllers to meet their direct obligations.

---

<sup>10</sup> Kate Goodloe, Why the Controller-Processor Distinction Matters to Privacy, Business Software Alliance (November 8, 2022), <https://techpost.bsa.org/2022/11/08/why-the-controller-processor-distinction-matters-to-privacy/>.

<sup>11</sup> Business Software Alliance, Controllers and Processors: A Longstanding Distinction in Privacy (October 12, 2022), <https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy>.

For example, processors are contractually obligated to provide functionality within their services that enable controllers to honor consumer requests to access or delete their personal information. When Salesforce provides our software to our customers, we operate as a data processor, handling customer data on behalf of and pursuant to the instructions of those customers.

**Encouraging Utilization of First Party Data**

Companies shouldn't rely on third-party ad tech companies and third-party cookies to learn about their customers. Rather, we believe utilizing first party data obtained directly from customers is the best approach for customer engagement because this data exchange is known and expected by the customer, opens up the possibility for direct communication, and allows companies to build trusted relationships with customers through effective and transparent personalization. For example, marketers and salespeople can use a unified view of their first party data to honor an individual's contact preferences across internal systems and give the individual easy-to-use controls to manage and update their preferences. Customer success departments (who help customers implement and get the most out of their purchases) can be aware of recent purchases and tailor their support accordingly. Business departments can recognize what a person likes about a product to provide a personalized experience or enable internal development teams to determine what new features to prioritize.

Companies have more data than ever, and it's imperative that they're able to integrate it, analyze it, and understand it - in a trusted and secure way. In an environment where a majority of individuals feel like they've lost control over how their data is used but still expect personalized experiences and engagement, these intentional first party interactions can build trust by delivering relevant, personalized interactions to individuals who have chosen to share their data.

For example, individuals should be empowered to provide companies with clear instructions on how their data can be shared and used to create a better customer experience.

U.S. law should encourage these sorts of first party engagements. Such an approach is in-line with global regulatory trends and market changes and would help to decrease reliance on less privacy protective third-party tracking techniques. It also allows consumers to more easily and effectively exercise their individual privacy rights. If consumers understand which companies process their data and how it will be used, they know who to contact to exercise their rights in a meaningful way.

#### **IV. Conclusion**

Congress has made great strides toward passing a comprehensive federal privacy law. Last year, this committee passed ADPPA by a resoundingly bipartisan vote of 53-2. 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.

ADPPA not only lines up well against the global standard envisioned first by the US with the HEW report and effectuated by GDPR, but it would return the U.S. to its global leadership role, especially on impactful issues like algorithmic impact assessment, application of civil rights to data protection, and restriction of third-party targeted advertising.

Thanks to decades of work and the significant advancements made last Congress, 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.

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 5 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:]



**Written Testimony of Amelia Vance**

**Founder and President, Public Interest Privacy Center**

**Before the US House Subcommittee on Innovation, Data, and Commerce**

**“Addressing America’s Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans’ Personal Information”**

Thursday, April 27, 2023

Chair Bilirakis, Ranking Member Schakowsky, and Members of the Committee:

It is an honor to testify before you on the need for better child and student privacy protections. I am the President and Founder of the Public Interest Privacy Center (PIPC) and an adjunct professor of law at William & Mary Law School. I also run the Student and Child Privacy Center, housed at AASA, The School Superintendents Association. PIPC is a pending nonprofit that equips stakeholders with the insights, training, and tools needed to cultivate effective, ethical, and equitable privacy safeguards for all children and students.

The child and student privacy legal and practical landscape is undergoing rapid, continual change. While educators and school administrators grapple with understanding and applying new technologies and data sharing practices within the classroom, new child privacy protections are being introduced in federal and state legislation on an almost-weekly basis. Since 2014, over 140 state laws have been passed that attempt to close these gaps. What has resulted is a confusing, dense, and insufficient legal landscape that leaves parents thinking that their children are protected or that there are no laws at all. And, worse, the chaos and legal gaps leave children and students vulnerable to serious harm.

In my work over the past decade, I have worked on student and child privacy with parents, local and state education agencies, researchers, privacy advocates, civil rights advocates, data use

proponents, and state and federal policymakers. These stakeholder groups can (and have) clashed regarding the appropriate balance of the use of data with sufficiently protecting privacy, but they all agree: current sectoral privacy protections are not sufficient to protect student privacy.

Today, I will share some of what I have learned in my work in this space, provide a brief overview of the current child and student privacy landscape, outline why children and students are particularly vulnerable to privacy risks, describe how current laws fall short in protecting children and students from privacy harms, and how a comprehensive consumer privacy bill could help close these gaps and create more safeguards for students and children.

### **Lay of the Land**

Child and student privacy legal protections currently exist through a layered, often outdated, and hard to navigate patchwork of federal and state laws. The Children's Online Privacy Protection Act (COPPA) contains significant protection gaps. For example, it only applies to information *from* children under the age of 13 - a surprise to many parents who think it applies to all information about their children - and most of COPPA's protections can be, and often are, easily waived. The Family Educational Rights and Privacy Act (FERPA) provides additional privacy protections for students, but is particularly hard to understand and apply due to the additional rules that exist in statute, regulation, guidance, and other sources of law. Like COPPA, FERPA also includes significant gaps in privacy protections; while education technology is now used for attendance, personalized learning, student counseling, and other educational and administrative purposes, those companies are not directly regulated under FERPA; schools bear the burden of ensuring big tech's compliance, absent a state law. The state legal landscape is evolving at a near-impossible to follow rate, making it hard for stakeholders, including parents, schools, and companies, to understand and navigate.

Today, there is almost universal agreement among parents, educators, and policymakers at both the federal and state levels that children and students deserve better privacy protections. The next step must be to unite decision makers' understanding of what the current laws are, what gaps remain in the current legal landscape, what additional risks need to be addressed, what the possible legislative solutions are, and how to best implement those solutions without restricting children and student's access to safe online communities and opportunities.

Given this legal landscape and the vulnerabilities that remain, child and student privacy laws are long overdue for modernization and clarity, especially in light of the rapid rate of emerging technologies. However, just expanding those protections are not enough; our children deserve and need privacy protections both the day before *and* the day after they turn 18. A carefully and well-informed, comprehensive federal privacy law could help close these gaps and provide the safeguards that children and students have long-needed. However, we also know children are uniquely vulnerable to certain harms, and it is also important to create heightened protections that safeguard children from risks unique to them.

### Children, Students, and Privacy Risks

Because students—especially younger children—are not fully equipped to weigh the potential benefits and risks of data collection and use, are more socially and physically vulnerable than adults, and lack experience in navigating social norms and knowing when to trust, they require special privacy protections. They also need to be protected from the more acute harms they are vulnerable to, such as opportunity loss and identity theft, that may not fully emerge until later in life.

Without proper safeguards, students' lives and futures may be irreparably altered by privacy invasions. Over the past decade, I've found that the concerns that are most often shared from parents, educators, policymakers, and students themselves can be categorized in the following ways:

Risk	Definition	How these concerns might be raised
Health & Safety	Personal or otherwise sensitive information may be revealed that could endanger students.	Is a stranger or someone dangerous able to communicate with my child or learn where my child lives?
Over-Collection & Over-Surveillance	Over-collection and monitoring of student data and online activity can have chilling effects on students.	How much information is being collected about my child?
The Permanent Record	Records of events, specifically mistakes, may be retained	Will my child's mistakes be recorded forever?

	indefinitely, potentially leading to detailed profiles that negatively impact students' future opportunities.	
Loss of Opportunity	Student data can be used to make decisions about students and, specifically, can result in denials of opportunity.	What information will be used to make determine which opportunities my child doesn't have access to?
Equity Concerns	Students have varying access to devices or internet service, has implications for safeguards in place and monitoring that occurs.	What if the information is biased? What if it is used in an inequitable way?  What if my child and I can't or don't have access to the information or technology?
Age-inappropriate Content	Students may access inappropriate websites and online content.	Is my child accessing content that isn't appropriate?
Social Harm	Revelation of personal and sensitive student information can result in stigmatization and cyberbullying.	Is my child being cyberbullied or stigmatized?
Commercialization	Companies may use student data to target students with advertisements and to build student profiles.	Are companies selling my child's data or targeting advertising to them?

Whether these risks are based on student privacy being violated or just the perception that it could be, these risks are generally what underpins child and student privacy controversies and dictates the content of child and student privacy laws, regulations, and policies. The perception of unethical or irresponsible practices due to misinformation or inadequate communication can result in a loss of trust, particularly in the student privacy context.

When we don't properly safeguard against these risks, it can result in disastrous outcomes for students that can last long after they graduate. For example, recent data breaches in

[Minneapolis](#) and [Los Angeles](#) school districts revealed sensitive information of both current and former students, including student disciplinary and health records. While increasing data security is one method of protecting against data breaches, minimizing the data that is collected in the first place and creating processes for deleting data when no longer needed can lessen the impact of these types of breaches.

The vast amount of data collected about children also poses a unique risk to children, potentially impacting their mental health, physical safety, and future opportunities. Especially in school, many children are unaware what is monitored and who may have access to their information. For example, a national [survey](#) indicated that school monitoring negatively impacts student mental health because students are concerned about expressing their opinions or seeking out resources out of fear that their searches, identities, and opinions may be revealed to others without their consent. Students' sensitive information could be better protected by limiting this type of data from being collected, restricting who has access to the data, and providing students and parents with transparent policies.

Often, current child privacy law permits almost all protections of childrens' data to be waived by consent. This is a problem because companies face few restrictions on using data after receiving parental consent. For example, parents may rush through or not read a privacy notice and consent to their child's data being collected without understanding the potential consequences. Consent is not a panacea for adequate privacy protections: consent mechanisms alone may be insufficient if students and parents do not fully comprehend what they are consenting to due to the form in which the information is conveyed, or if students' opportunities to engage in learning or activities is conditioned on use of certain tools. Many educational activities take place without consent, and, in the educational context, obtaining meaningful consent might not be feasible. Therefore, it is vital for law to include underlying privacy protections that cannot be overridden by consent or that require a higher standard of consent where the risks are clear and consent is better informed, in order to protect the privacy and retain the trust and goodwill of students, parents, and educators.

These harms are certainly concerning for any parent and may spark a knee-jerk reaction that entails keeping their kids offline all together. However, in this day and age, robust technology use is not only a reality, but also a necessity in order to prepare young adults to navigate a digital world. Let's not forget that there are also many benefits that technology has provided for children. Unable to connect with their friends and communities in-person during the pandemic,



young people relied on social media and other online tools to play, build community, explore their identities, and participate in civic and political forums. Many educational technology (EdTech) tools play a valuable and innovative role in a child's learning, digital citizenship prepares them for the adult world, and safe online interactions with their peers can create a vital sense of community. Online spaces can also be integral to fostering creative expression and providing resources related to health and well-being.

Allowing opportunities for youth online while mitigating risks is no small endeavor; it is entwined with children's well-being today and their opportunities tomorrow. In the same way we teach our children to look both ways before crossing the street, we must equip kids to make good privacy decisions for themselves. The most basic way technology changes society is through the choices that we make- the choices that *our children* make - about which technologies we adopt and reject, and how to wisely use the ones that are selected.

The current legal landscape, consisting of both federal and state level laws, does not adequately address these risks. While providing some privacy protections, significant gaps still remain.

### **Legal Landscape**

#### *Federal Laws*

The Family Educational Right and Privacy Act of 1974 (FERPA) provides students with access to and transparency regarding their education records, and limits disclosure of education records by educational institutions to certain, limited circumstances listed in the statute. However, FERPA has a critical gap in privacy protections. FERPA applies only to schools, and therefore its restrictions and requirements only apply directly to schools, and not to private sector organizations, including EdTech companies. However, EdTech companies can be indirectly regulated under FERPA. EdTech companies are generally only regulated by FERPA so far as the contract between the school and EdTech company includes FERPA protections - something that is often a difficult burden for small schools to negotiate into contracts on their own.

In addition to FERPA, children's data is protected via the Children's Online Privacy Protection Act (COPPA), which restricts "online operators" from collecting data from children under the age of 13 without obtaining verifiable parental consent. COPPA generally only applies to online operators who target their services to children or who have actual knowledge they are collecting

information from children. As you can imagine, this actual knowledge standard creates a confusion about whether or not data collection on many sites is actually covered. COPPA also does not provide any substantive rights to children or their parents regarding the data collected.

COPPA's only protection is to apply restrictions to data collection (by requiring consent) but once the data is collected, the company has no restrictions under COPPA to how it must use, process, or share, or refrain from using, processing, or sharing the data, and it does not afford any rights in the data.

There is also massive confusion around and problematic gaps in FERPA and COPPA's protections depending on where and for what reason an app is being used by a child: if an educational app is being used in the classroom or at the direction of a teacher for homework, the data being collected is generally protected under FERPA. However, the moment that that child starts playing with that educational app for fun or at their parents' behest, FERPA ceases to apply. At that point, it would be great if COPPA covered that gap; however, since COPPA allows parents to waive many of its protections via parental consent, parents may not realize that their child is now unprotected under both FERPA and COPPA.

Misunderstandings about the intersection of FERPA and COPPA also creates problems. For example, some EdTech companies have begun to shift their COPPA responsibilities for obtaining verifiable parental consent to schools, even though companies, not education institutions, are subject to and responsible for complying with the law. Lack of clarity on the intersection between the two laws has resulted in confusion, diffusion of responsibility, and evasion.

#### *State student privacy laws and child privacy*

Since 2013, policymakers have introduced nearly one-thousand student privacy bills in all 50 states, and 41 states and Washington, DC, have enacted more than 130 laws, whose scope and effectiveness vary by state. Unfortunately, state-level student data privacy laws have been fragmented and variable, creating robust student data privacy protections in some states and insufficient protections. We've seen well-intentioned laws that have critical loopholes, and others that go too far and have overly-restrictive unintended consequences, which negatively impact student success and well-being.

For example, Louisiana passed a law that required parents to return a consent form to share any student data. Children of parents who forgot to return the form or chose not to, were

excluded from consideration from the state scholarship fund. New Hampshire similarly passed a law with good intentions but negative unintended consequences when it banned the recording of classroom lessons. Classroom recordings are sometimes necessary for students with learning disabilities so they have the resources necessary to keep up with their peers. In an attempt to protect students, New Hampshire inadvertently took this resource away from the students who need it most.

As I noted in my Seton Hall Legislative Journal article, “Student Privacy’s History of Unintended Consequences,” many state level laws “were passed hastily in response to public fears or specific incidents, with little stakeholder input. Others neglected to clearly define the scope and requirements of the laws, resulting in confusion and anxiety.” These state experiences with passing, implementing, and fixing student privacy laws may be valuable in informing the process of improving consumer privacy protections.

*State consumer privacy laws and child privacy*

Utah’s law includes children’s privacy within its definition of “sensitive personal information,” and states that controllers (covered businesses) may not “process sensitive personal data without “processing the data in accordance with” COPPA. If you are a covered business under Utah who collects information from children, but are not an online operator (or, if you have a website but don’t collect data through your website), this is puzzling, because you are not required to process data “in accordance with” COPPA or to obtain parental consent since you are not an online operator. Similarly, Virginia’s law also includes data collected from individuals under 13 in its definition of sensitive data, and requires businesses to not process “sensitive data concerning a known child, without processing such data in accordance with” COPPA. Like Utah, this is a bit confusing, because not all businesses that are covered under the VCDPA that collect/process child data are required to comply with COPPA. Accordingly, for businesses that are not online operators within COPPA’s purview, collecting data “in accordance with” COPPA would likely look like normal data collection with no heightened protection, which undermines the purpose of these laws.

As mentioned above, these provisions are not always effective, and can be confusing, since COPPA only applies to online operators and the state consumer privacy laws apply to all businesses, regardless of how they collect information. Virginia and Utah’s laws (and they are not alone) demonstrate both a misconception, and a gap when examining how state consumer privacy laws protect (or do not protect) children. The requirements in these laws seemingly try to

create a heightened collection standard when it comes to child data, similar to the heightened standard (often opt-in, rather than opt-out consent) required to collect health data, biometric data, and other similarly sensitive data, but by tying this collection standard to COPPA, which only applies in the limited context of online data collection, it does not afford the robust protection it may appear to at first brush. Legislators need to remember that not all businesses are required to comply with COPPA, so the requirements to collect data in accordance with COPPA can be confusing or ineffective.

Finally, the safe harbor offered under some state laws (such as Virginia's) which deem businesses who "comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.)" to be in compliance with "any obligation to obtain parental consent" under the law may be more workable to blend COPPA and existing state law together in a way that understands what protections COPPA is already affording and where it does not afford protections.

Some of FERPA and COPPA's gaps are also filled by state consumer privacy laws that are being introduced and passed throughout the country and affording consumers in states who have passed such laws baseline privacy rights. Beyond simply being notice and consent regimes, which is largely what COPPA is and which often does not facilitate meaningful privacy protections, these state laws go a step beyond and provide more substantive, baseline rights to individuals.

The baseline rights appearing in state consumer privacy laws generally include the right to access information, the right to know what information is being collected, the right to delete information under certain circumstances, the right to opt-out of certain uses of information (such as using information for cross-context behavioral advertising or targeted advertising), and certain rights regarding sensitive personal information (such as the requirement for the business to obtain opt-in consent prior to collection or consent for certain uses of sensitive personal information). When these laws include new child privacy protections, they generally do so by placing COPPA-like restrictions on information collection from individuals under the age of 13, by providing safe harbors for companies that collect information "consistent with COPPA's requirements," or by including information of or related to individuals under the age of 13 in the definition of sensitive personal information.

Since these laws are based on a common misconception of COPPA's breadth, they do not adequately fill the gaps that exist under current law. However, because these laws apply to all

individuals and do not set a floor for the age at which a consumer gains rights under the statutes (i.e., only afford individuals over 18 rights under the statute), these laws provide some additional protection to children via the substantive rights they afford to all consumers. Other than requiring notice of the company's privacy practices, and the right to review information collected (and in some instances, prevent further use), COPPA does not afford children (or parents on behalf of their children) significant rights in their data post-collection.

Another way that state consumer privacy laws tend to contemplate children is by including information of or related to individuals under the age of 13 in the definition of sensitive personal information. This means that the additional protections afforded to sensitive personal information under the law, which most often include opt-in rather than opt-out consent to collect and to use data for certain purposes, applies to children's data. In some ways, this is more protective than COPPA since COPPA only applies to information collection, and does not afford meaningful substantive rights or meaningfully restrict use or collection after consent to collection.

Some state consumer privacy laws say that if you are compliant with COPPA's verifiable parental consent (VPC) requirements then you also meet the requirements of the state law. However, the application of VPC can also be problematic. Obtaining VPC often involves using age verification methods, which can be easily circumvented by children. When applied, VPC may also lead to "age gating" the Internet and attempting to block certain content from children (which again, can be easily circumvented) instead of simply making the content more appropriate for audiences that may include children or younger individuals.

Instead of relying on restrictive systems that require opt-ins and parental consent, some states are moving toward a system where privacy protections are designed into the sites they expect children to visit.

*Moving Away from Notice and Consent to Underlying Protections: The Age Appropriate Design Code*

In one of the first meetings of the [OECD](#)'s expert working group to revise their recommendation on protecting children online, Baroness Beeban Kidron presented about the Age Appropriate Design Code (AADC) and put forth the question (paraphrased here) "What if kids didn't have to lie on the internet to be protected but also get access to services?" The AADC is designed to enable children to do just that. It is built upon implementing additional safeguards that allow children to use the internet in an age- and developmentally-appropriate way.

When introduced in 2020, the United Kingdom adopted the AADC, a detailed set of fifteen non-prescriptive standards “[seek\[ing\] to protect children within the digital world, not protect them from it.](#)” The code establishes the [following fifteen standards](#) as a framing through which companies implement age appropriate design into their online services: best interests of the child; data protection impact assessments; age appropriate application; transparency; detrimental use of data; policies and community standards; default settings; data minimisation; data sharing; geolocation; parental controls; profiling; nudge techniques; connected toys and devices; online tools.

The EU’s General Data Protection Regulation (GDPR) served as a foundation upon which the AADC is built. As explained in the [Information Commissioner’s foreword](#) to the final Code, “The code is not a new law but it sets standards and explains how the [GDPR] applies in the context of children using digital services.” This is a crucial point: the AADC’s enhanced protections for children are based upon the foundation of privacy protections for everyone. These enhanced protections for children elevated the baseline protections to be more effective at protecting children because they accounted for children’s unique vulnerabilities and need for additional protections. The US also needs a comprehensive privacy law upon which to build out additional protections for children.

The AADC includes various privacy safeguards by design and default to make the internet a safer place for children. For example, it protects the privacy of children’s location data by requiring geolocation data collection be turned off by default in most circumstances and that geolocation be turned back on after a child has turned it on. It emphasizes just-in-time notifications to ensure that children are aware of what is happening while they are using the internet. It also prohibits the [use of dark patterns](#) to the detriment of children; limits profiling a child by default; requires businesses to think carefully and document decision-making about the privacy impacts of their services that are likely to be accessed by children; and calls for privacy policies to be available in terms that children can understand. Many of these child privacy protections should be represented in US privacy law, and not just to protect children.

#### **Child Privacy-Specific State Laws**

As with student privacy, policymakers have also attempted to close sectoral privacy law gaps by introducing additional state-level child privacy laws.

*The U.S. Version of the Age-Appropriate Design Code*

Following California's groundbreaking consumer privacy laws, California decided to innovate on child privacy too. Building off of the UK's AADC, the California Age-Appropriate Design Code Act (ADCA) mandates that businesses, as defined under the California Consumer Privacy Act/California Privacy Rights Act ([CCPA/CPRA](#)), implement increased privacy protections by design for online services likely to be accessed by children. These laws are based on the acknowledgement that online engagement is a reality and baseline protections must be in place. UNICEF's "[Growing up in a Connected World](#)" report demonstrates this reality. They report that across the world, one in every 3 people online are kids and teens.

The ADCA requires covered businesses to either "estimate the age of child users with a reasonable level of certainty appropriate to the risks" or to "apply the privacy and data protections afforded to children to all consumers." This requirement alone has the potential to transform how everyone, including adults, experiences the internet. As was seen with the CCPA/CPRA, because of California's size and market power and because of the breadth of the law, even with its threshold requirements, this law could change online practices for companies throughout the US because of California's market power and size. The law may also raise the baseline standard for everyone who uses the internet or online resources because if businesses can't find a way to accurately identify children, the ADCA will effectively require them to treat everyone accessing their websites as a child, which resets the baseline and could result in content restrictions, limitations on personalization, and limited functionality for all website users, when these restrictions may only be appropriate for certain content that is unsafe for children.

However, some states are choosing a more restrictive approach, passing laws that place significant restrictions on certain websites and mobile apps, such as social media platforms, related to child users of these platforms, following the example of other countries like [China](#) and South Korea. For example, Utah's law applies to minors under the age of 18, and limits how and when children can use social media by setting a curfew that prohibits evening or early morning access, and requires parental consent for use, gives parents broad rights regarding access to accounts, and places use restrictions on social media companies related to children including prohibiting social media companies to display ads to children, target or suggest groups, products, posts, or services to children, and prohibiting the use of addictive design with child users.

[While this law was passed with good intentions](#), blocking the internet from children instead of teaching them how to safely use the internet, or making the internet safer, would have more

beneficial impacts, particularly since children historically figure out ways to bypass or circumvent age gates and access the content without consent (and in this case, past curfew). The law also treats all individuals under the age of 18 the same way, which overlooks that content that is safe and potentially beneficial for a 16 to 18-year-old is different from the content that is safe and beneficial for a four year old.

South Korea's law may actually be a case study in the problems with this approach. When South Korea passed the "Shutdown law" that banned children under the age of 16 from playing computer games between midnight and 6am, their government was, similarly to current U.S. concerns had some similar concerns to what we are hearing in the US now: worries about "[internet addiction](#)" that so bad, in some cases, that it led to people neglecting themselves or their children to "[the point of death](#)." The paternalistic law [did not allow](#) parents the flexibility to choose to allow their child to play. However, South Korea repealed the law in 2021, choosing a more balanced approach that allows parents and guardians to "arrange approved play times" instead. South Korean Deputy Prime Minister and Education Minister said that, "In the changing media environment, the ability of children to decide for themselves and protect themselves has become important more than anything," and the government would, instead, "work with related ministries to systematically support media and game-use education at schools, homes, and in society so that young people can develop these abilities, and continue to make efforts to create a sound gaming environment and various leisure activities for children."

Other bills have proposed overly restrictive requirements that fail to consider the potential impact on schools and children. For example, some proposed solutions inadvertently undermine the goals of a bill by including censorship mechanisms restricting access to certain content. These may discourage minors from seeking help and finding helpful resources that include personal stories from peers. Overly restrictive proposals may also undermine the abilities of schools to provide education using technology.

When it comes to safeguarding our children online, we commonly use two approaches. The first, encouraging our kids to wear their virtual seatbelts and take steps to stay safe while online. The second approach is to avoid the internet entirely or limit access only to occasions where there is parental supervision. Unfortunately, both approaches have significant drawbacks. They involve numerous gaps, can be easy for kids to get around, inappropriately place the onus on parents to adequately vet a technology's privacy practices, or rely on a large amount of additional data collection about families. These approaches also fail to adequately deal with



additional risks, such as commercial exploitation of their data and excessive government surveillance.

### **A Comprehensive Law**

Comprehensive consumer privacy laws provide necessary baseline privacy protections for all consumers, including children. By providing blanket rights for all consumers, we help close many of the privacy gaps in child and student privacy laws and make technology use much safer and beneficial for children. In the same way, the UK's AADC would not be effective if it were not based on the EU's general consumer protection code, the General Data Protection Regulation (GDPR).

While providing baseline privacy rights for all consumers, a general consumer privacy law does not completely close the gaps in child and student privacy laws. Since it does not fully address the specific child privacy risks that we have laid out and for that reason, additional privacy protections for children are necessary.

Businesses must also be transparent about what data they collect, how they use it, and how individuals can exercise their afforded rights. Transparency is a fundamental principle in many privacy laws, particularly because a lot of privacy laws are premised on the concepts of notice and consent. Transparency makes consumer consent more meaningful because consumers have clear notice. However, transparency may not be enough to ensure children are protected online.

The current model for providing transparency - namely, providing a privacy notice - requires individuals, including children, to be willing and able to engage with the organization's privacy information (source: [Data protection impact assessments](#)). In reality, children (and even some adults) will not read an entire privacy notice regardless of whether it is transparent and written in an understandable way. To ensure children are protected even if they do not engage with transparent privacy policies online, additional safeguards are needed. These additional safeguards may include measures such as meaningful use restrictions and limitations specifically targeted to alleviate specific harms to children, as discussed above, or additional processing restrictions including mandatory DPIAs before processing any child information.

Certain information processing activities pose different risks and harms to children than to adults, and it is important to recognize and account for additional potential impacts on children. Conducting Data Protection Impact Assessments (DPIAs) and Algorithm Impact Assessments

(AIAs) can help identify and assess a variety of risks, including risks that are unique to children. The UK Information Commissioner's Office (ICO's) DPIA framework set forth in the AADC lends a helpful framework, identifying several child-focused risks and potential impacts, specifically saying to consider "whether the processing could cause, permit, or contribute to the risk of: physical harm; online grooming or other sexual exploitation; social anxiety, self-esteem issues, bullying or peer pressure; access to harmful or inappropriate content; misinformation or undue restriction on information; encouraging excessive risk-taking or unhealthy behaviour [sic]; undermining parental authority or responsibility; loss of autonomy or rights (including control over data); compulsive use or attention deficit disorders; excessive screen time; interrupted or inadequate sleep patterns; economic exploitation or unfair commercial pressure; or any other significant economic, social or developmental disadvantage." Due to the additional vulnerabilities of children, it is crucial that considering the likelihood and severity of potential risks and harms of processing on children at all ages and development stages is built into the evaluation process of online technologies in addition to the considerations for all consumers in a comprehensive law.

Once potential risks and harms to children have been identified through DPIAs and AIAs, those risks and harms can then be addressed with appropriate mitigation measures to better protect children. Additional security requirements, including mandated training and appointment of privacy and security officers, can be implemented to protect the rights of children. Data minimization requirements and additional protections for sensitive data, such as requiring affirmative express consent before transferring sensitive data about and from children, are especially critical to protect children from the potential negative impacts of collecting large amounts of sensitive data about and from children.

A comprehensive consumer privacy law should prohibit businesses from using manipulative design choices (dark patterns) to obscure or impair people's ability to exercise their rights. Dark patterns (referred to as "nudge techniques" in the AADC) can cause individuals, including children, to reveal more information than they would have if a website or platform did not push them to share additional information.

Children face additional unique risks from dark patterns when compared to adults. For example, dark patterns encouraging children to overshare personal information online may result in cyberbullying and dark patterns encouraging continued use of social media may result in amplified mental harms due to the tendency of children to be more susceptible to comparing

themselves to others or viewing themselves under a microscope. Additionally, nudge techniques that encourage children to provide unnecessary personal data or to turn off privacy protective controls so that organizations can collect additional data from them goes against data minimization principles and can create a larger dossier of information related to children that can follow them for the rest of their lives.

However, manipulative design techniques can also benefit kids by gently encouraging them to stay engaged with healthy, productive, and learning-based content. For example, dark patterns or nudge techniques used in certain contexts may encourage children to share information that supports their health and wellbeing with appropriate parties to act on that information. Another potentially beneficial nudge specifically applicable to children may be techniques that encourage children to pause their activity online and step away from technology without losing progress to promote taking breaks in periods of uninterrupted screen time. In certain contexts, manipulative design techniques can be utilized in positive ways to promote childrens' wellbeing, encourage healthy habits, and encourage kid's engagement in productive activities. Because manipulative design techniques may benefit children when used appropriately, a comprehensive privacy bill should not ban them entirely. Rather, businesses should be restricted from using these techniques to keep individuals from exercising their rights, such as opting out of data collection.

A comprehensive and carefully crafted consumer data protection law can also add protections against entities and data practices less often considered to be harmful by regulating non-profits. Including non-profit organizations is useful for filling the gaps left by many existing sectoral privacy laws that do not apply to non-profit organizations.

A comprehensive consumer privacy law can also better protect data used for research. For background, many types of research—including education research—are controlled by Institutional Review Boards, which ensure that research is ethical and data is protected. However, Institutional Review Boards are rarely equipped to evaluate privacy and security risks. Ideally, a comprehensive consumer privacy law could help remedy this gap by requiring additional privacy and security specific guidelines for research, with special attention to projects that are exempt from the review process.

In addition to raising privacy protections for all consumers, a comprehensive consumer privacy bill can carve out additional protections for children that fill the gaps in existing legislation. The law would ideally apply these additional protections when the covered entity knows the

individual is under 17, without carving out different knowledge standards for some social media companies and large data holders.

Prohibiting targeted advertising to minors is a useful protection that can be provided by a comprehensive privacy bill. California's law provides this protection by allowing all consumers regardless of their age to limit the use of the "sale" and "sharing" of their data (with the "sale" and "sharing" of data generally understood to encompass the practice of targeted advertising). Specifically, California graduates the protections in this space by requiring opt-in consent from parents of children younger than 13 and directly from individuals age 13-16 in order to "sell" or "share" their personal information, and by allowing individuals over age 16 to opt-out of this practice.

Companies using targeted advertising exploit children's data to manipulate their decision-making to buying products or services, a particularly dangerous practice due to the increased vulnerability of children. This prohibition also fills gaps left by COPPA, where targeted ads are not prohibited as long as the provider has parental consent to collect and process a child's data. Additionally, the prohibition on transferring minor's data to third parties absent affirmative consent gives minors and parents control over how their data is used and limits the ability to use data for secondary purposes beyond what the data was originally collected for.

Among the provisions that require additional protections for minors, requiring large data holders to conduct yearly algorithm impact assessments that must describe, among other things, how the entity will mitigate harms specific to minors could be extremely beneficial. Requiring yearly algorithmic impact assessments to assess and mitigate potential harms to minors is a powerful tool to ensure that large data holders will think about the needs and specific vulnerabilities of children in designing and continuing to provide access to their services in safer ways for children. Entities must acknowledge the unique potential risks of algorithms to minors and plan accordingly to mitigate those harms.

Additionally, a comprehensive consumer privacy bill can create additional resources at the FTC dedicated to children and minor's privacy, including requiring the FTC to promulgate new COPPA rules and funding a new Youth Privacy and Marketing Division. The FTC has limited resources to dedicate to protecting children because they are responsible for [over 70 different laws](#). Adding a new division dedicated to children is useful to ensure compliance with ADPPA and its minor specific provisions.

Finally, rights provided to individuals are only meaningful if they can be enforced. A comprehensive consumer privacy law can fulfill this requirement by including a private right of action for individuals to enforce their rights. A private right of action provides specific benefits to children by filling gaps in existing legislation. Parents and children cannot sue businesses that violate COPPA and must rely on the FTC and state attorney generals to enforce their rights. A comprehensive consumer privacy bill that includes a private right of action gives parents, children, and all consumers more control over their data by allowing them to enforce their rights against businesses that fail to protect them.

*Including Special Protections in a Comprehensive Consumer Privacy Law for Education*

While it's the best next step in protecting children and students, it's important to note that a comprehensive consumer privacy bill on its own doesn't provide all the protections we'd like to see for children and students. Consumer privacy might not clearly address the relationship between schools and companies.

In the education context, consent is often not useful. Much student data collection, use, and sharing is involuntary: children are required to attend school, where they participate in activities that generate new data about them, such as completing online homework assignments. Under FERPA, schools are permitted to consent on behalf of parents—assuming specific privacy safeguards are in place—to enable nearly every aspect of tech-supported education, from keeping attendance records to grading exams. If this changed, any student whose parents have objected would likely be unable to use EdTech. Teachers may have to choose between creating and implementing multiple lesson plans for the same classroom or not using EdTech at all. This change would leave teachers not only ill-equipped to teach in a modern environment, but also coping with post-pandemic challenges like [learning loss](#) with resources of the 1980's. It is important to protect the ability of schools to use technology as core curriculum—the digital equivalent of a textbook—without permitting opt-outs. However, in order to ensure that companies are adequately protecting privacy, additional safeguards tailored to the education context are necessary. Even where consent may be appropriate, students and parents are often not in the best position to assess the benefits and risks of data collection and use; the burden of vetting the technology used by their child's school should not be placed on them.

One way to fix this is to include a federal version of the prominent state student privacy law regulating vendors, SOPIPA, in a comprehensive consumer privacy law. For example, a draft bill introduced by Representatives Polis and Messer in 2015 included the necessary nuance to deal

with privacy in the education context, and was endorsed by most major education groups and the National PTA.

### **Conclusion**

Children and students face many specific and acute privacy risks in this digital age. Despite policymakers' best attempts, we currently have a patchwork system of laws and protections that do not sufficiently protect children and students. Significant gaps remain in the federal laws and state laws are not successfully closing those gaps. A broader, general consumer-based approach, coupled with additional child-specific provisions, could be an effective best next step forward and a way to ensure that all children and students benefit from the opportunities provided by emerging technologies in a safer, more privacy-protective way.

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 5 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. OK. 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 5 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 healthcare 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 [continuing]. Should avoid?

Mr. REED [continuing]. 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 oftentimes 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 healthcare 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 5 minutes.

Mrs. RODGERS. 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's 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 superinteresting 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.

Mrs. RODGERS. 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.

Mrs. RODGERS. OK.

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

Mrs. RODGERS. OK, thank you.

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

Mrs. RODGERS. 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.

Mrs. RODGERS. 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 5 minutes of questioning.

Ms. Kelly, I didn't see Ms. Kelly. Ms. Kelly, I will recognize you for your 5 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 healthcare 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 healthcare providers, healthcare 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—5 minutes to Dr. Bucshon.

You are recognized for your 5 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 [continuing]. 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 [continuing]. 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 [continuing]. 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 healthcare is the way to move.

Mr. BUCSHON. OK. As I said, the—even some of the EU people who we talked 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 5 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



X's 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.

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 5 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 appears at the conclusion of the hearing.]

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 oftentimes 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 Kids 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's 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.

OK. 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 5 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 policymakers, 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. OK. 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. OK. 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—refiled 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's 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 one 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 5 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 displayed.]

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 cybersecurity 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 as-

sessments. 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 5 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 2 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 multibillion-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 5 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 sophis-

tication 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, followup, 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. OK. 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's 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 5 minutes of questioning.

You are recognized.

Mrs. DINGELL. Thank you, Mr. Chairman. And I want you to know the NLF 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 popups. 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 popup. 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 overcollection 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 5 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 5 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—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 hyperspecialized 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 5 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 [continuing]. 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 compli-

ance 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 5 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 36th time Congress has had a hearing on the—on privacy in the last 5 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 5 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 followup 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 Cali-

ifornia 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 underestimated 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 5 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 appears at the conclusion of the hearing.]

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.]

[Material submitted for inclusion in the record follows:]



**Subcommittee on Innovation, Data, & Commerce**  
**Hearing entitled “Addressing America's Data Privacy Shortfalls: How A National**  
**Standard Fills Gaps To Protect Americans' Personal Information”**  
**[April 27, 2023]**

**Documents for the record**

At the conclusion of the meeting, the chair asked and was given unanimous consent to include the following documents into the record:

1. A Washington Post article entitled, “Remote learning apps shared children’s data at a ‘dizzying scale,’” May 24, 2022, submitted by Representative Walberg.
2. A letter from the National Association of Federally-Insured Credit Unions, April 26, 2023, submitted by the Majority.
3. A letter from the California Privacy Protection Agency, April 26, 2023, submitted by the Minority.
4. A letter from Privacy for America, April 27, 2023, submitted by the Minority.
5. A letter from leading members of the U.S. startup ecosystem, April 27, 2023, submitted by the Minority.
6. A report from the Information Technology and Innovation Foundation entitled, “The Looming Cost of State Privacy Laws,” January 2022, submitted by the Majority.
7. A letter from the Credit Union National Association, April 27, 2023, submitted by the Majority.
8. A statement for the record from U.S. PIRG, April 27, 2023, submitted by the Minority.
9. Written testimony from Mr. Edmund Mierzewski to the Committee on Financial Services, February 26, 2019, submitted by the Minority.

## TECHNOLOGY

# Remote learning apps shared children's data at a 'dizzying scale'

The educational tools used by students during the pandemic shared their information with advertisers and data brokers that could track them around the Web, an international investigation found



By [Drew Harwell](#)

May 24, 2022 at 9:00 p.m. EDT

Millions of children had their online behaviors and personal information tracked by the apps and websites they used for school during the pandemic, according to an international investigation that raises concerns about the impact remote learning had on children's privacy online.

The educational tools were recommended by school districts and offered interactive math and reading lessons to children as young as prekindergarten. But many of them also collected students' information and shared it with marketers and data brokers, who could then build data profiles used to target the children with ads that follow them around the Web.

Those findings come from the most comprehensive study to date on the technology that children and parents relied on for nearly two years as basic education shifted from schools to homes.

Researchers with the advocacy group [Human Rights Watch](#) analyzed 164 educational apps and websites used in 49 countries, and they shared their findings with The Washington Post and 12 other news organizations around the world. The consortium, EdTech Exposed, was coordinated by the investigative nonprofit [the Signals Network](#) and conducted further reporting and technical review.

What the researchers found was alarming: nearly 90 percent of the educational tools were designed to send the information they collected to ad-technology companies, which could use it to estimate students' interests and predict what they might want to buy.

Researchers found that the tools sent information to nearly 200 ad-tech companies, but that few of the programs disclosed to parents how the companies would use it. Some apps hinted at the monitoring in technical terms in their privacy policies, the researchers said, while many others made no mention at all.

The websites, the researchers said, shared users' data with online ad giants including Facebook and Google. They also requested access to students' cameras, contacts or locations, even when it seemed unnecessary to their schoolwork. Some recorded students' keystrokes, even before they hit "submit."

The "dizzying scale" of the tracking, the researchers said, showed how the financial incentives of the data economy had exposed even the youngest Internet users to "inescapable" privacy risks — even as the companies benefited from a major revenue stream.

"Children," lead researcher Hye Jung Han wrote, were "just as likely to be surveilled in their virtual classrooms as adults shopping in the world's largest virtual malls."

School districts and the sites' creators defended their use, with some companies saying researchers had erred by including in their study homepages for the programs, which included tracking codes, instead of limiting their analysis to the internal student pages, which they said contained fewer or no trackers. The researchers defended the work by noting that students often had to sign in on the homepages before their lessons could begin.

The coronavirus pandemic abruptly upended the lives of children around the world, shuttering schools for more than 1.5 billion students within the span of just a few weeks. Though some classrooms have reopened, tens of millions of students remain remote, and many now depend on education apps for the bulk of their school days.

Yet there has been little public discussion of how the companies that provided the programs remote schooling depends on may have profited from the pandemic windfall of student data.

The learning app Schoology, for example, says it has more than 20 million users and is used by 60,000 schools across some of the United States' largest school districts. The study identified code in the app that would have allowed it to extract a unique identifier from the student's phone, known as an advertising ID, that marketers often use to track people across different apps and devices and to build a profile on what products they might want to buy.

A representative for PowerSchool, which developed the app, referred all questions to the company's privacy policy, which said it does not collect advertising IDs or provide student data to companies for marketing purposes. But the policy also says the company's website uses third-party tools to show targeted ads to users based on their "browsing history on other websites or on other devices." The policy did not say which third-party companies had received users' data.

The policy also said that it “does not knowingly collect any information from children under the age of 13,” in keeping with the [Children’s Online Privacy Protection Act](#), or COPPA, the U.S. law that requires special restrictions on data collected from young children. The company’s software, however, is marketed for classrooms as early as kindergarten, which for many children starts around age 4.

The investigation acknowledged that it could not determine exactly what student data would have been collected during real-world use. But the study did reveal how the software was designed to work, what data it had been programmed to seek access to, and where that data would have been sent.

School districts and public authorities that had recommended the tools, Han wrote, had “offloaded the true costs of providing education online onto children, who were forced to pay for their learning with their fundamental rights to privacy.”

The researchers said they found a number of trackers on websites common among U.S. schools. The website of [ST Math](#), a “visual instructional program” for prekindergarten, elementary and middle school students, was shown to have shared user data with 19 third-party trackers, including Facebook, Google, Twitter and the e-commerce site [Shopify](#).

Kelsey Skaggs, a spokeswoman for the California-based [MIND Research Institute](#), which runs [ST Math](#), said in a statement that the company does not “share any personally identifiable information in student records for the purposes of targeted advertising or other commercial purposes” and does not use the same trackers on its student platform as it does on its homepage.

But the researchers said they found trackers not just on [ST Math](#)’s main site but on pages offering math games for prekindergarten and the first grade.

Google spokesperson [Christa Muldoon](#) said the company is investigating the researchers’ claims and will take action if they find any violations of their data privacy rules, which include bans on personalized ads aimed at minors’ accounts. A spokesperson for Facebook’s parent company, Meta, said it restricts how businesses share children’s data and how advertisers can target children and teens.

The study comes as concern grows over the privacy risks of the educational-technology industry. The Federal Trade Commission [voted](#) last week on a [policy statement](#) urging stronger enforcement of COPPA, with Chair [Lina Khan](#) arguing that the law should help “ensure that children can do their schoolwork without having to surrender to commercial surveillance practices.”

COPPA requires apps and websites to get parents’ consent before collecting children’s data, but schools can consent on their behalf if the information is designated for educational use.

In an announcement, the FTC said it would work to “vigilantly enforce” provisions of the law, including bans against requiring children to provide more information than is needed and restrictions against using personal data for marketing purposes. Companies that break the law, it said, could face fines and civil penalties.

Clearly, the tools have wide impact. In Los Angeles, for example, more than 447,000 students are using Schoology and 79,000 are using ST Math. Roughly 70,000 students in Miami-Dade County Public Schools use Schoology.

Both districts said they've taken steps to limit privacy risks, with Los Angeles requiring software companies to submit a plan showing how student information will be protected while Miami-Dade said it had conducted a "thorough and extensive" evaluation process before bringing on Schoology last year.

The researchers said most school districts they examined had conducted no technical privacy evaluations before endorsing the educational tools. Because the companies' privacy policies often obscured the extent of their monitoring, the researchers said, district officials and parents often were left in the dark on how students' data would be collected or used.

Some popular apps reviewed by the researchers didn't track children at all, showing that it is possible to build an educational tool without sacrificing privacy. Apps such as Math Kids and African Storybook didn't serve ads to children, collect their identifying details, access their cameras, request more software permissions than necessary or send their data to ad-tech companies, the analysis found. They just offered simple learning lessons, the kind that students have relied on for decades.

Vivek Dave, a father of three in Texas whose company RV AppStudios makes Math Kids, said the company charges for in-app purchases on some word-search and puzzle games designed for adults and then uses that money to help build ad-free educational apps. Since launching an alphabet game seven years ago, the company has built 14 educational apps that have been installed 150 million times this year and are now available in more than 35 languages.

"If you have the passion and just try to understand them, you don't need to do all this level of tracking to be able to connect with kids," he said. "My first beta testers were my kids. And I didn't want that for my kids, period."

The researchers argued that governments should conduct data-privacy audits of children's apps, remove the most invasive, and help guide teachers, parents and children on how best to prevent data over-collection or misuse.

Companies, they said, should work to ensure that children's information is treated differently from everyone else's, including by being siloed away from ads and trackers. And lawmakers should encode these kinds of protections into regulation, so the companies aren't allowed to police themselves.

Bill Fitzgerald, a privacy researcher and former high school teacher who was not involved in the study, sees apps' tracking of students not only as a loss of privacy but as a lost opportunity to use the best of technology for their benefit. Instead of rehashing old ways to vacuum up user data, schools and software developers could have been pursuing fresher, more creative ideas to get children excited to learn.

"We have outsourced our collective imagination and our vision as to what innovation with technology could be to third-party product offerings that aren't remotely close to the classroom and don't have our best interests at heart," Fitzgerald said.

“The conversation the industry wants us to have is: What’s the harm?” he added. “The right conversation, the ethical conversation is: What’s the need? Why does a fourth-grader need to be tracked by a third-party vendor to learn math?”

Abby Rufer, a high school algebra teacher in Dallas, said she’s worked with a few of the tested apps and many others during a frustratingly complicated two years of remote education.

School districts felt pressured during the pandemic to quickly replace the classroom with online alternatives, she said, but most teachers didn’t have the time or technical ability to uncover how much data they gobbled up.

“If the school is telling you to use this app and you don’t have the knowledge that it might be recording your students’ information, that to me is a huge concern,” Rufer said.

Many of her students are immigrants from Latin America or refugees from Afghanistan, she said, and some are already fearful of how information on their locations and families could be used against them.

“They’re being expected to jump into a world that is all technological,” she said, “and for many of them it’s just another obstacle they’re expected to overcome.”



3138 10th Street North  
Arlington, VA 22201-2149  
703.522.4770 | 800.336.4644  
f: 703.524.1082  
nafcu@nafcu.org | nafcu.org

**National Association of Federally-Insured Credit Unions**

April 26, 2023

The Honorable Gus M. Bilirakis  
Chairman  
Committee on Energy and Commerce  
Subcommittee on Innovation, Data,  
and Commerce  
U.S. House of Representatives  
Washington, DC 20515

The Honorable Janice D. Schakowsky  
Ranking Member  
Committee on Energy and Commerce  
Subcommittee on Innovation, Data,  
and Commerce  
U.S. House of Representatives  
Washington, DC 20515

**Re: Tomorrow's Hearing: "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information"**

Dear Chairman Bilirakis and Ranking Member Schakowsky:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) ahead of tomorrow's hearing, "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 135 million consumers with personal and small business financial service products. NAFCU and our members welcome the Subcommittee's review of this important issue.

As NAFCU has previously communicated to Congress, we believe there is an urgent need for comprehensive federal data privacy legislation that protects consumer data, establishes data safeguards, and recognizes the standards that have been in place for over two decades with the Gramm-Leach-Bliley Act (GLBA). In 2019, recognizing the importance of data privacy and the ongoing privacy debate, NAFCU issued a series of data privacy principles that calls for a comprehensive federal cybersecurity standard, the harmonization of existing federal data privacy laws, and the preemption of state privacy laws. As the Subcommittee works to develop much-needed comprehensive federal data privacy legislation, NAFCU recommends you include the following elements as key aspects in any such proposal:

- **A comprehensive federal cybersecurity standard covering all entities that collect and store consumer information.** Uniformly strong cybersecurity is necessary to ensure Americans' data is adequately protected across the economy. Existing strong federal cybersecurity standards, like that contained in the GLBA, should be extended to the activities of all data collectors and processors exceeding certain reasonable thresholds.
- **Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.** The current patchwork of federal and state data privacy laws generates incredible consumer

The Honorable Gus M. Bilirakis  
 The Honorable Janice D. Schakowsky  
 April 26, 2023  
 Page 2 of 4

confusion and significant compliance burdens while failing to address the most significant data privacy risks to Americans—those risks posed by unregulated or inconsistently regulated entities that collect, control, and process vast amounts of our data. Comprehensive federal data privacy legislation should responsibly build on the successes of robust, time-tested federal laws by extending the same robust data privacy standards across the economy and ensuring that already well-regulated entities, like credit unions, may confidently operate within their existing federal frameworks without fear of being subject to more than 50 different data privacy and security standards.

- **Delegation of enforcement authority to the appropriate sectoral regulator.** The National Credit Union Administration (NCUA) should be federal credit unions' sole data privacy and cybersecurity regulator. Allowing the NCUA, which is well-versed in the unique nature of federal credit unions and their operations, to continue to examine and enforce any privacy and cybersecurity requirements is the most efficient option for both credit unions and American taxpayers. Exposing credit unions and other already well-regulated entities to suits by states' attorneys general and private rights of action will dramatically increase compliance costs without providing a corresponding increase in consumer protection.
- **A safe harbor for businesses that take reasonable measures to comply with the privacy standards.** Comprehensive federal data privacy legislation should adopt principles-based requirements based on an organization's specific operations and risk profile and include a safe harbor for organizations that design and implement appropriate measures.
- **Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.** Providing multiple data privacy disclosures and opt-out mechanisms across multiple channels creates consumer confusion and unreasonable burdens for subject entities. A new privacy law should avoid conflicting or duplicative disclosure requirements by incorporating easy to understand language, like that consistent with the GLBA's disclosure requirements.
- **Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.** Actual damages to consumers are too difficult to establish by evidence, and statutory damages for violations are incredibly ripe for frivolous lawsuits. Sectoral regulators alone should have the power to assess scalable civil penalties, which can then be used to remedy and prevent consumer harm in a meaningful way.



The Honorable Gus M. Bilirakis  
 The Honorable Janice D. Schakowsky  
 April 26, 2023  
 Page 3 of 4

While NAFCU supports a national data security and privacy standard, we had some concerns about the American Data Protection and Privacy Act (ADPPA) that the Energy and Commerce Committee considered in the last Congress, including:

- *GLBA Exemption.* Through the GLBA, Congress defined robust federal data privacy and information security standards for the financial services industry and provided the NCUA and other federal financial regulators the means to create and maintain strong privacy and data safeguards. The ADPPA did not recognize these long-standing requirements by providing a GLBA exemption. Congress should recognize the strength and successes of the GLBA and other time-tested federal sectoral data privacy regulation, and the value of regulator-led regulation, by wholly exempting credit unions and other already closely-regulated entities.
- *Private Right of Action.* This legislation provided a private right of action which would allow individuals or states' attorneys generals to sue covered entities over potential violations allowing courts to determine the law. This means that different judicial interpretations will allow a consumer in California to have different privacy protections than a consumer in South Carolina, and credit unions will find themselves immediately and unnecessarily exposed to new and substantial compliance and legal risks.
- *Preemption of State Laws.* The ADPPA would preempt many state laws but then subsequently provided exceptions that undermine the preemption. This would perpetuate a patchwork of state and federal data privacy legislation and regulation. We believe Congress must leverage comprehensive federal data privacy legislation to expressly preempt all state data privacy legislation and regulation.

As your colleagues on the House Financial Services Committee tackle the Data Privacy Act, H.R. 1165, within its jurisdiction to improve the GLBA for financial services entities, we urge the Subcommittee to craft a workable GLBA expansion to those outside of financial services that may be handling consumer financial data. The GLBA has successfully served consumers, credit unions, and other covered financial institutions for nearly a quarter-century. Changes to the GLBA for those already covered by it must be viewed with a cautionary eye. While some modernization of the GLBA for financial institutions may be in store, the system has generally been a success and should be a model for other areas. Making the system work best means expanding financial data protection requirements outside of just financial services. Retailers, merchants, and others that handle financial data should be subject to new requirements similar to those standards adopted for financial institutions. We urge the Subcommittee to work with your counterparts on the House Financial Services Committee to ensure a balance that recognizes existing law and the concerns of credit unions as Congress tackles the important issue of privacy reform.

The Honorable Gus M. Bilirakis  
The Honorable Janice D. Schakowsky  
April 26, 2023  
Page 4 of 4

NAFCU looks forward to continuing to work with you to address these concerns with consumer privacy. On behalf of our nation's credit unions and their more than 135 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information, please contact me or Lewis Plush NAFCU's Senior Associate Director of Legislative Affairs, at 703-842-2836 or [lplush@nafcu.org](mailto:lplush@nafcu.org).

Sincerely,

A handwritten signature in black ink that reads "Brad Thaler". The signature is written in a cursive, flowing style.

Brad Thaler  
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Innovation, Data, and Commerce

**CALIFORNIA PRIVACY PROTECTION AGENCY**

2101 Arena Blvd  
 Sacramento, CA 95834  
[www.cppa.ca.gov](http://www.cppa.ca.gov)



April 26, 2023

The Honorable Gus Bilirakis, Chair  
 The Honorable Jan Schakowsky, Ranking Member  
 Innovation, Data, and Commerce Subcommittee  
 House Energy & Commerce Committee  
 United States House of Representatives  
 Washington, DC 20515

**Re: Innovation, Data, and Commerce Subcommittee Hearing: “Addressing America’s Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans’ Personal Information”**

Dear Chair Bilirakis and Ranking Member Schakowsky:

The California Privacy Protection Agency (Agency)<sup>1</sup> writes to thank the Innovation, Data, and Commerce Subcommittee for highlighting the importance of protecting the privacy and security of personal information not currently covered by privacy laws in its hearing, “Addressing America’s Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans’ Personal Information.”<sup>2</sup> But such protections should not come at the expense of existing rights. H.R. 8152, the American Data Privacy and Protection Act (ADPPA),<sup>3</sup> which the Agency opposes in its current form, seeks to significantly weaken the protections currently in place in the states, including safeguards Californians currently enjoy under the California Consumer Privacy Act, as amended (CCPA).<sup>4</sup> Instead, lawmakers should support legislation that sets a federal floor and encourages states to continue to take the lead to advance protections.

Supporting states’ efforts to adopt legislation to address their own residents’ needs is consistent with interoperability. For example, the CCPA directs the Agency to work with policymakers in other jurisdictions to ensure consistency in privacy protections.<sup>5</sup> And the Agency’s CCPA regulations were carefully crafted to not contravene a business’s compliance with other privacy laws, such as Europe’s General Data Protection Regulation (GDPR) and consumer privacy laws recently passed in Colorado,

<sup>1</sup> Established by California voters in 2020, the California Privacy Protection Agency was created to protect Californians’ consumer privacy. The Agency implements and enforces the California Consumer Privacy Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.

<sup>2</sup> United States House of Representatives, Innovation, Data, and Commerce Subcommittee Hearing: “Addressing America’s Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans’ Personal Information” (April 27, 2023), <https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-addressing-america-s-data-privacy-shortfalls-how-a-national-standard-fills-gaps-to-protect-americans-personal-information>.

<sup>3</sup> H.R. 8152 (2022), <https://www.congress.gov/bills/117/congress/house-bill/8152/text>.

<sup>4</sup> Cal. Civ. Code § 1798.100 et seq.

<sup>5</sup> *Id.* § 1798.199.40(i).

Virginia, Connecticut, and Utah.<sup>6</sup> In addition to working with other jurisdictions to ensure consistent protections, the Agency is also in regular contact with state, federal, and international regulators to help ensure consistent enforcement of the law.

Nearly all federal privacy laws already allow states to adopt stronger protections, which California has done. Such additional protections have not prevented California from becoming one of the world's leading economies.<sup>7</sup> For example, The Health Information Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA), and the Fair Credit Reporting Act (FCRA) all contain language that allow the states to adopt stronger protections.<sup>8</sup> The Telephone Consumer Protection Act (TCPA) and the Video Privacy Protection Act (VPPA) also allow for stronger state laws.<sup>9</sup> California has already adopted stronger protections in many of these areas, from the Confidentiality of Medical Information Act (CMIA), which is similar to, but broader than, HIPAA, and the California Financial Information Privacy Act (CFIPA), which was explicitly adopted to provide a higher standard of protections than GLBA.<sup>10</sup>

Furthermore, it's not clear that the ADPPA will create a single national standard, a purported justification for the bill's preemption language.<sup>11</sup> ADPPA seeks to preempt swaths of existing state privacy laws but allows covered businesses to develop their own compliance plans, to be submitted to the FTC for approval.<sup>12</sup> This safe harbor could lead to hundreds if not thousands of different compliance standards, causing confusion among consumers seeking to exercise their rights. This could be particularly harmful to members of underserved communities that do not have the resources to navigate these varying procedures.

The ADPPA could certainly weaken existing protections. For example, the CCPA gives Californians significant protections with respect to automated decision-making (ADM), including the right to access meaningful information about the logic involved in automated decisions and the right to opt out of automated decision-making.<sup>13</sup> This would enable California to help rein in algorithms, such as those used by social media apps popular with young adults and children that play a role in targeting harmful

<sup>6</sup> California Privacy Protection Agency, California Consumer Privacy Act Regulations, Notice of Proposed Rulemaking (July 8, 2022), [https://cppa.ca.gov/regulations/pdf/20220708\\_npr.pdf](https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf).

<sup>7</sup> Office of Governor Gavin Newsom, *ICYMI: California Poised to Become World's 4th Biggest Economy* (Oct. 24, 2022), <https://www.gov.ca.gov/2022/10/24/icymi-california-poised-to-become-worlds-4th-biggest-economy/>.

<sup>8</sup> See 45 C.F.R. Part 160, Subpart B; 15 U.S.C. § 6807; 15 U.S.C. § 1681t.

<sup>9</sup> 47 U.S.C. § 227(f); 18 U.S.C. § 2710(f).

<sup>10</sup> Cal. Civ. Code § 56.10 et seq.; Cal. Fin. Code § 4051(b).

<sup>11</sup> Memo, from Committee Majority Staff, to Members, Subcommittee on Innovation, Data, and Commerce, re: Hearing Entitled "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information" (Apr. 25, 2023), [https://d1dth6e84htgma.cloudfront.net/IDC\\_Memo\\_American\\_Data\\_Privacy\\_Hearing\\_2023\\_04\\_27\\_1\\_bda35f1b5d.pdf?updated\\_at=2023-04-25T21:40:51.125Z](https://d1dth6e84htgma.cloudfront.net/IDC_Memo_American_Data_Privacy_Hearing_2023_04_27_1_bda35f1b5d.pdf?updated_at=2023-04-25T21:40:51.125Z).

<sup>12</sup> See Sec. 303-4.

<sup>13</sup> Cal. Civ. Code § 1798.185(a)(16).

content,<sup>14</sup> or generative AI and Large Language Models that are growing in popularity at an astronomical rate, which ADPPA does not address.

The ADPPA also seeks to prevent the states from strengthening privacy protections in the future. ADPPA was introduced before the Dobbs decision created new urgency for meaningful privacy protections.<sup>15</sup> Since ADPPA was introduced, California has already adopted new laws to protect reproductive privacy, including a bill that, among other provisions, prevents out-of-state law enforcement entities from obtaining information from California businesses about an abortion that would be legal in California.<sup>16</sup> This year, the California legislature is also considering a bill to protect data collected by certain reproductive health apps by the CMIA<sup>17</sup> and a bill that would restrict the tracking of consumers near family planning centers, among others.<sup>18</sup> Washington State appears poised to advance HB 1155, a reproductive privacy law with sweeping protections over this sensitive data. In contrast, ADPPA has not been meaningfully amended to address new concerns with respect to reproductive privacy.

Ten state attorneys general, including those in Illinois and New Jersey, criticized ADPPA's preemption language, and "encourage[d] Congress to adopt legislation that sets a federal floor, not a ceiling, for critical privacy rights and respects the important work already undertaken by states to provide strong privacy protections for our residents."<sup>19</sup> California Governor Newsom, Attorney General Bonta, Assembly Speaker Anthony Rendon, and members of the California Senate have also raised concerns about preemption language in the ADPPA.<sup>20</sup>

ADPPA represents a false choice: that strong federal protections must come at the expense of the states. Americans deserve both, a federal floor that allows states to adopt stronger protections. We look forward to working with you to promote and safeguard these protections.

<sup>14</sup> Ben Smith, *How Tik Tok Reads Your Mind*, N.Y. Times (Dec. 5, 2021), <https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html>.

<sup>15</sup> See, e.g., Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info in Pregnant People*, Politico (Aug. 1, 2022), <https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988>.

<sup>16</sup> 2022 Cal. Stat. 89 (AB 1242).

<sup>17</sup> AB 254 (2023).

<sup>18</sup> SB 345 (2023).

<sup>19</sup> Letter from Ten Attorneys General to Congressional Leaders (July 19, 2022), <https://oag.ca.gov/system/files/attachments/press-docs/Letter%20to%20Congress%20re%20Federal%20Privacy.pdf>.

<sup>20</sup> Letter from Governor Newsom, Attorney General Bonta, and the California Privacy Protection Agency to Congressional Leaders (Feb. 28, 2023), [https://cippa.ca.gov/pdf/adppa\\_letter.pdf](https://cippa.ca.gov/pdf/adppa_letter.pdf); Letter from California Assembly Speaker Rendon to U.S. House Speaker Nancy Pelosi (July 19, 2022), [https://cippa.ca.gov/meetings/materials/20220728\\_item2\\_letter\\_assembly\\_speaker.pdf](https://cippa.ca.gov/meetings/materials/20220728_item2_letter_assembly_speaker.pdf); Letter from Senator Tom Umberg et al. to U.S. House Speaker Nancy Pelosi (Aug. 9, 2022).

130

Sincerely,

Ashkan Soltani  
Executive Director

Cc: The Honorable Cathy McMorris Rodgers, Chair  
The Honorable Frank Pallone, Jr., Ranking Member  
Members, House Energy & Commerce Committee



April 27, 2023

The Hon. Cathy McMorris Rodgers  
Chair  
House Energy & Commerce Committee  
2125 Rayburn House Office Building  
Washington, D.C. 20515

The Hon. Gus Bilirakis  
Chairman  
House Energy & Commerce  
Subcommittee on Innovation, Data, and  
Commerce  
2306 Rayburn House Office Building  
Washington, D.C. 20515

The Hon. Frank Pallone  
Ranking Member  
House Energy & Commerce Committee  
2322 Rayburn House Office Building  
Washington, D.C. 20515

The Hon. Jan Schakowsky  
Ranking Member  
House Energy & Commerce  
Subcommittee on Innovation, Data, and  
Commerce  
2408 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chair Rodgers, Chairman Bilirakis, Ranking Member Pallone, and Ranking Member Schakowsky:

Privacy for America is a coalition of trade organizations and companies representing a broad cross-section of the American economy. Our membership includes companies and trade associations in the advertising, travel, hospitality, media, financial services, data services, market research, and many other industries. We have long urged the creation of a single comprehensive, preemptive national standard for consumer privacy that supplements the existing set of sectoral and anti-discrimination laws already in effect in the United States.

As the House Energy and Commerce Committee Innovation, Data, and Commerce Subcommittee's ("Subcommittee") considers an approach to this type of comprehensive, preemptive law in its hearing on "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information," the Subcommittee should take a risk-based approach to such a law and balance consumer protection with the responsible use of data. This balance was absent from the American Data Privacy Protection Act ("ADPPA") as it stood at the end of the last Congress. We write to highlight several facts that we urge the Subcommittee to seriously consider during this hearing and its work going forward in an effort to appropriately calibrate a preemptive, comprehensive national privacy law for business and consumers across the United States.

- **Sectoral and anti-discrimination laws work to address data practices within their purview.** For decades the United States has maintained robust protections for data industries including health care, financial services, telecommunications, and education. It has also built up strong defenses against the misuse of data related to certain protected classes, including protections for children's data and protections against the use of data to discriminate against individuals in housing, credit, and employment based on characteristics



like race and gender. These long-standing laws, with long histories of enforcement and complex compliance programs within responsible companies, should not be left by the wayside as Congress assesses how to address the modern data-driven economy.

- **The Privacy for America Framework provides the model approach for privacy legislation.** The Subcommittee can look to the Privacy for America *Principles of Privacy Legislation* (“Framework”) as an example of how to strike an appropriate balance for national data standards.<sup>1</sup> The Framework defines certain uses of personal information as reasonable and others as per se unreasonable and thus prohibited.<sup>2</sup> The Framework prioritizes consumer protection while also allowing consumers and businesses alike to derive immense value from reasonable uses of data and access to a vibrant online ecosystem.
- **Congress should set a national standard when addressing potential gaps in privacy protections and not abdicate that power to the Federal Trade Commission.** When the Subcommittee considers approaches to a comprehensive privacy law to supplement the sectoral laws, a bedrock principle of that work must be to set a true, preemptive national standard. The regulation of the modern data-driven economy is best left to the democratically accountable legislative branch, not individual states or executive branch agencies. Personal data is collected and processed almost exclusively in interstate commerce and, accordingly, should be subject to a single national standard, not a patchwork of differing state statutes. Data collection and processing, therefore, should be established once through the clear authority granted to Congress by the American people and the Constitution.
- **Private companies should follow the law, not create their own.** When Congress creates a true national framework for data practices, no company should be allowed to interfere in the legitimate, responsible, data practices Congress has authorized. Just because one entity maintains a market position as an intermediary between consumers and publishers does not give it the right to prevent otherwise legally permissible and responsible data processing. This concern is especially true when those private actors choose to obstruct reasonable data flows in order to further their own financial goals to the inevitable detriment of their competitors. A federal law should ban such meddling.
- **Responsible data-driven practices deliver over \$30,000 in value to each consumer per year.** Any comprehensive national privacy law needs to balance the costs to consumers and businesses against the increased consumer protections such a law may offer. And the costs of overzealous regulation could be immense, as studies have found that companies’ data-driven practices keep \$30,000 per year in the pockets of each consumer in the United States thanks to free and discounted entertainment, information, and other services.<sup>3</sup> Congress

<sup>1</sup> Privacy for America, *Principles for Privacy Legislation* (2019) <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/>.

<sup>2</sup> Framework at Part I, Sec. 1(Y); Sec. 3: Sec 6(G)(c).

<sup>3</sup> J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 2 (2022), <https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf>.





should not reach into consumer's bank accounts by imposing unreasonable restrictions on the data services companies that provide the backbone of many of these free and low-cost services that consumers desire. Consumers do not deserve a new \$30,000 tax.

\* \* \*

Thank you for your consideration of this letter on this important topic. We look forward to working with you as you continue to evaluate and develop approaches to preemptive, comprehensive, national privacy legislation that will properly balance consumer protection and the vital, efficient, and effective data-driven practices required for a growing and dynamic United States economy.

Sincerely,  
Privacy for America

April 27, 2023

The Honorable Frank Pallone  
Ranking Member  
Committee on Energy and Commerce  
2322 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers  
Chair  
Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Maria Cantwell  
Chair  
Committee on Commerce, Science,  
and Transportation  
254 Russell Senate Office Building  
Washington, D.C. 20510

The Honorable Ted Cruz  
Ranking Member  
Committee on Commerce, Science,  
and Transportation  
512 Dirksen Senate Office Building  
Washington, D.C. 20510

Dear Chair Rodgers, Ranking Member Pallone, Chair Cantwell and Ranking Member Cruz:

As leading members of the U.S. startup ecosystem—entrepreneurs, startup founders, incubators, investors, accelerators, and support organizations—located in 26 states that serve individuals, businesses, schools, and governments in every state across the country and throughout the world, we write to urge you to pass a uniform, consistently-enforced, comprehensive data privacy law to create certainty for us and provide baseline protections for our customers.

We are creating new ways for individuals to learn critical skills, helping people to advance in their careers, assisting businesses in reducing emissions, improving health outcomes for at-risk populations, among so many other innovative contributions to advance society. We care deeply about our users, customers, and clients, respect their privacy, and invest heavily in keeping their data safe.

Unfortunately, the rapidly shifting landscape of state privacy laws makes it difficult for us to be confident that we are compliant with the letter of each law and leads us to spend considerable time and resources navigating these disparate, complex frameworks. In fact, new research shows that we each spend hundreds of thousands and forgo up to 20% of revenue on often duplicative compliance activities.<sup>1</sup> A uniform federal privacy framework would create clarity for us, streamline these costs, allow us to better serve our customers, and improve our competitiveness all while ensuring that our customers in each state have the same privacy protections. The resources we save could be put toward hiring more workers to grow our businesses, investing in R&D to improve our products, and supporting our communities.

<sup>1</sup> *Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startups*, Engine (Mar. 24, 2023), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6414a45f5001941e519492ff/1679074400513/Privacy+Patchwork+Problem+Report.pdf>.

Last Congress you came closer than ever to passing a federal privacy law. We encourage you to build on that momentum this Congress while keeping in mind the needs of startups. We need federal privacy law that:

**Creates uniformity.** Startups need a federal privacy law to preempt individual state privacy laws. Without preemption, a federal privacy law would merely be another law added to the patchwork and would not create certainty or ease compliance for us.

**Limits bad faith litigation.** A federal privacy law should be consistently enforced by expert agencies and limit opportunities for bad actors to exploit the high cost of privacy litigation to extract settlements from startups by bringing lawsuits even when startups have not violated the law.

**Respects the resources of startups.** Many of us have not yet raised formal funding rounds and instead rely on our personal savings or the revenue we generate. Even those of us that have raised outside capital have significantly fewer resources than our larger competitors. A federal privacy law must account for our resources and ability to comply.

**Accounts for the tools startups use.** We use multiple tools and services to build our companies. As you formulate a federal privacy law, you should keep in mind the interconnectedness of the startup ecosystem.

The startup community supports your efforts to create a uniform, consistently-enforced federal privacy framework to create clarity and establish protections for all Americans. We thank you for considering our views.

Sincerely,

1Huddle  
6AM City, Inc.  
Abstract  
Airpals Technologies Inc.  
Ardian Group, Inc.  
Availyst  
Bims Laboratories, Inc.  
Black & Brown Founders  
Boolean Girl  
Broadside Digital

Bryght Labs  
Carefully  
Center for American Entrepreneurship  
CitiQuants Corp.  
Connector Labs  
Courtam, Inc. dba People Clerk  
Cover  
Cranberry Queues Corp.  
DAF.Financial, Inc.  
Denver Angels

Ecobot	Lumo
Educreations	M1PR, Inc.
Engine	Max Borges Agency
Eskwad	Maxwell
Event Vesta, Inc	Onfleet, Inc.
Free From Market	PILOT Inc.
FundBlackFounders	PIE
Gaussian Holdings	Polyhedra
Global Response Systems	Productions.com
Globalfy, LLC	RAVN
Green Tech Coast	Raydiant Oximetry, Inc.
Gust	Red Cap Ventures
Hacom	Refraction, Inc.
hobbyDB	Renee
Hush	Right to Start
Infiltron Software Suite	Signals
Innovare	STY Holdings
Institute for Energy and Sustainability, Inc.	TaxCredit.ai
IronCore Labs, Inc.	TheraTec, Inc.
Libib	Tostie Productions, LLC
Linktree	Venntive LLC
ListedB	Voatz, Inc.
LiteraSeed, Inc.	WePower Technologies LLC

cc: Honorable Members of the House Committee on Energy and Commerce and the Senate Committee on Commerce, Science, and Transportation



Jim Nussle  
President & CEO

Phone: 202-508-6745  
jnussle@cuna.coop

99 M Street SE  
Suite 300  
Washington, DC 20003-3799

April 27, 2023

The Honorable Gus Bilirakis  
Chairman  
Energy and Commerce Subcommittee  
on Innovation, Data and Commerce  
United States House of Representatives  
Washington, DC 20515

The Honorable Jan Schakowsky  
Ranking Member  
Energy and Commerce Subcommittee  
on Innovation, Data and Commerce  
United States House of Representatives  
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

On behalf of America's credit unions, I am writing about your hearing "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans Personal Information". CUNA represents America's credit unions and their more than 135 million members.

Credit unions strongly support the enactment of a national data security and data privacy law that includes robust security standards that apply to all who collect or hold personal data and is preemptive of state laws. We firmly believe that there can be no data privacy until there is strong data security. Securing and protecting consumer data is important not only for their individual financial health but as a further safeguard against rogue international agents and interference by foreign governments.

Data privacy and data security are major concerns for Americans given the frequency of reports of misuse of personally identifiable information (PII) data by businesses and breaches by criminal actors, some of which are state sponsored. Since 2005, there have been more than 10,000 data breaches, exposing nearly 12 billion consumer records. These breaches have cost credit unions, banks, and the consumers they serve hundreds of millions of dollars, and they have compromised the consumers' privacy, jeopardizing their financial security.

Stringent information security and privacy practices have long been part of the financial services industries' business practices and are necessary as financial institutions are entrusted with consumers' personal information. This responsibility is reflected in the strong information security and privacy laws that govern data practices for the financial services industry as set forth in the Gramm Leach Bliley Act ("GLBA"). GLBA's protection requirements are strengthened by federal and state regulators' examinations for compliance with the GLBA's requirements and robust enforcement for violations. Several of these significant regulatory requirements and internal safeguards include:

- **Federal Requirements to Protect Information:** Title V of the GLBA and its implementing rules and regulations require credit unions to protect the security, integrity, and confidentiality of consumer information.
- **Federal Requirements to Notify Consumers:** Credit unions are required to notify their members whenever there is a data breach where the misuse of member information has occurred or where it is reasonably likely that misuse will occur.

[cuna.org](http://cuna.org)

- **Strong Federal Oversight and Examination:** Under their broad-based statutory supervisory and examination authority, the National Credit Union Administration (NCUA) and the Consumer Financial Protection Bureau (CFPB) regularly examine credit unions for compliance with data protection, privacy, and notice requirements.
- **Strong Federal Sanction Authority:** Under numerous provisions of federal law, credit unions are subject to substantial sanctions and monetary penalties for failure to comply with statutory and regulatory requirements.

While this extensive legal and regulatory examination and enforcement framework ensures that credit unions robustly protect consumers' personal financial information, this safety net only extends to financial institutions. As consumers' personal information is disseminated to third parties, those protections end and credit unions and their members are adversely impacted by the lax data security standards at other businesses. These loopholes must end and a comprehensive data security and privacy framework that covers all entities that collect consumer information and is preemptive of state laws must be established and this standard must hold those who jeopardize that data accountable through enforcement.

With that in mind, we ask the committee to consider the following data security and privacy principles for any comprehensive framework:

**New Privacy and Data Security Laws Should Keep GLBA Intact:** Congress should leave financial services' robust data and privacy requirements in place. Financial services and the healthcare industry are subject to federal data privacy laws. The GLBA and the Health Insurance Portability and Accountability Act (HIPAA) have protected American's PII for over two decades and should be left in place as financial services and healthcare and their respective regulators have developed regulations, guidance, and procedures for compliance.

**Data Privacy and Data Security Are Hand in Glove:** Any new privacy law should include both data privacy and data security standards. Simply put, data cannot be kept private unless it is also secured. Congress should enact robust data security standards to accompany and support data privacy standards.

**Every Business Not Already Subject to Federal Law Should Follow the Same Rules:** The new law should cover all businesses, institutions, and organizations. Consumers will lose if Congress focuses only on tech companies, credit-rating agencies, and other narrow sectors of the economy because any company that collects, uses, or shares personal data or information can misuse the data or lose the data through breach.

**There Should Be One Rule for the Road:** Any new law should preempt state requirements to simplify compliance and create equal expectation and protection for all consumers. We understand that some states have strong security and privacy requirements. Congress should carefully examine those requirements and take the best approaches from state law, as appropriate. A patchwork of state laws with a federal standard as a floor will only perpetuate a security system littered with weak links. The federal law should be the ceiling and the ceiling should be high. Just like moving away from the sector specific approach, the goal should be to create a strong national standard for all to follow.

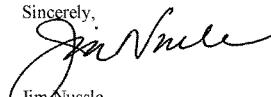
**Breach Disclosure and Consumer Notification Are Important, But These Requirements Alone Won't Enhance Security or Privacy:** Breach notification or disclosure requirements are important, but they are akin to sounding the alarm after the fire has burned down the building. By the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions, of individuals.

**Hold Entities that Jeopardize Consumer Privacy and Security Accountable Through Regulatory Enforcement:** The law should provide mechanisms to address the harms that result from privacy violations and security violations, including data breach. Increasingly, courts are recognizing rights of action for individuals and companies (including credit unions). However, individuals and companies should be afforded a private right of action to hold those that violate the law accountable, and regulators should have the ability to act against entities that violate the law.

**Recognize This Issue For What It Is – A National Security Issue:** More and more, data breaches that expose consumer PII are perpetrated by foreign governments and other rogue international entities. The proceeds from these attacks are being used to fund illicit activity. The nature of these breaches alone calls for a strong federal response that ensures all involved in collecting, holding, and using PII do so with the security of the information of paramount concern. You simply cannot have data privacy unless there is data security.

On behalf of America's credit unions and their more than 135 million members, thank you for your consideration of our views and for holding this important hearing.

Sincerely,



Jim Nussle  
President & CEO



April 27, 2023

The Hon. Gus Bilirakis  
Chairman  
House Energy & Commerce Subcommittee on Innovation, Data, and Commerce  
2306 Rayburn House Office Building Washington, D.C. 20515

The Hon. Jan Schakowsky  
Ranking Member  
House Energy & Commerce Subcommittee on Innovation, Data, and Commerce  
2408 Rayburn House Office Building Washington, D.C. 20515

Re: Hearing: "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information"

Dear Chairman Bilirakis and Ranking Member Schakowsky:

Attached please find U.S. PIRG's statement for the record for your hearing on "Addressing America's Data Privacy Shortfalls."

It describes the inherent danger in preempting the states on page 2 in greater detail. We also believe it would be a mistake to exempt all entities covered by the Gramm -Leach-Bliley Act from your legislation and would be happy to discuss this further. Please let me know if you have any questions.

Sincerely,

Ed Mierzewski  
Senior Director, Federal Consumer Program, PIRG  
edm@pirg.org



**Testimony of  
Edmund Mierzwinski**

**Senior Director, Federal Consumer Programs  
U.S. Public Interest Research Group**

---

**At a Hearing On**

**Who's Keeping Score? Holding Credit Bureaus  
Accountable and Repairing a Broken System**

**Before the U.S. House of Representatives  
Committee on Financial Services**

**The Honorable Maxine Waters, Chairwoman**

---

**26 Feb 2019**

Chairwoman Waters, Mr. McHenry, members of the committee. My name is Edmund Mierzwinski, Senior Director for Federal Consumer Programs at the U.S. Public Interest Research Group, which serves as the federation of state PIRGs, which are member-based, non-profit, non-partisan research and advocacy organizations around the country.

### **1. Summary**

Thank you for the opportunity to testify today on the important matter of Fair Credit Reporting Act (FCRA) reform. The law was passed in 1970 and has been amended over the years. It regulates the activities of consumer reporting agencies (CRAs), commonly called credit bureaus. What is a CRA, or credit bureau? We like one court's description of the behemoth Experian as a "company that traffics in the reputations of ordinary people."<sup>1</sup>

We have prepared a rough timeline of some major consumer reporting problems that have led to state or federal policymaker reforms and enforcement actions by the Federal Trade Commission or Consumer Financial Protection Bureau. The list also includes enforcement actions by state attorneys general and consumer protection attorneys, who each play a critical role in reining in the CRAs. The timeline is attached as an appendix to this report. We hope it is helpful and I can answer questions about any of its items.

I first testified before this committee<sup>2</sup> on credit reporting mistakes in 1989, at a time when several states and the Federal Trade Commission (FTC) were conducting investigations and negotiating consent decrees with several large consumer reporting agencies<sup>3</sup> due to a troubling pattern of consumer complaints over both their mistakes and their recalcitrance and failure to correct the mistakes after consumers exercised FCRA-mandated dispute rights.

That 1989 hearing was the first real effort by Congress to rein in the credit bureaus since passage of the original act in 1970. Since then, Congress has continually conducted oversight and, in response to industry's indifference to the problems it causes for consumers seeking financial or employment opportunity, has enacted significant reforms in 1996, 2003 and 2010.

---

<sup>1</sup> See <https://caselaw.findlaw.com/us-9th-circuit/1209375.html>

<sup>2</sup> House Banking Committee, Subcommittee on Consumer Affairs and Coinage, Hearings on Fair Credit Reporting, 13 Sept 1989. (After the Gramm-Leach-Bliley Act of 1999, the full committee's name was changed to Financial Services Committee.)

<sup>3</sup> "Credit bureau" is a widely used colloquial term for Consumer Reporting Agencies regulated under the Fair Credit Reporting Act (FCRA) 15 U.S.C. § 1681 *et seq.* The so-called Big 3 bureaus, Equifax (formerly Retail Credit Company), Experian (formerly TRW) and TransUnion now qualify as Nationwide Consumer Reporting Agencies (15 U.S.C. § 1681a(p)) and face greater responsibilities under the act. Many other firms, including specialty CRAs offering check cashing and bounced check databases, employment background checks, tenant screening, medical insurance and other services are regulated under the act's definitions. However, the Big 3 continue to grow, with their recent acquisitions of competitors: for example, Experian acquiring Clarity Services, Equifax buying DataX and TransUnion buying FactorTrust, all in the last few years. The 3 smaller firms fashion themselves as alternative databases operating in the subprime space.

*States Lead the Way*

Critically, each federal reform was preceded by major accomplishments at the state level. A key part of my message today is that continued state leadership in all areas – from climate change to credit reporting and privacy and digital rights more broadly – is critical to the advancement of this nation’s policies to improve consumer welfare, health and safety and liberty.

Numerous states emulated California’s pioneering auto emissions rules, protecting the environment for us and future generations. As you know, those state rules are currently under administrative threat. The pioneering 2018 California Consumer Privacy Act is now under attack in the Commerce committees of both houses by a phalanx of powerful corporate interests led by Google, Facebook, Amazon and the telco/cable ISPs. If they win preemption of state laws, consumers and citizens lose, forever.

The big CRAs were early advocates of eliminating the right of states to protect their citizens. If the credit bureaus and banks had succeeded **in 1992** in their brazen House effort to reverse the FCRA’s longstanding standard that the FCRA serve as a floor of protection, not a ceiling, and at that time 27 years ago successfully preempted all state laws related to credit reporting, we would not have nationwide free credit reports, we would not have access to our credit scores, we would not have identity theft protections, we would not have data breach notices, and we would not have the free nationwide credit freezes finally enacted in 2018.<sup>4</sup> Congress only acts to protect consumers after a disaster (cue 2008 financial collapse) or after several states act first. Industry’s goal is to take state innovators and consumer cops off the credit bureau beat.

In this testimony, in addition to detailing the need for consumer reporting reform, we call on Congress to ensure that Equifax finally pays a price for its massive 2017 data breach affecting over 148 million consumers.

**Finally, we offer our strong support to the two draft bills from Chairwoman Waters and other members, which are before the committee today.** The first, a new version of the Chairwoman’s Comprehensive Consumer Credit Reporting Reform Act, is a response to the problems posed to all consumers by the failure of the consumer reporting system. That system is dominated by its Big 3 members – Experian, Equifax, and TransUnion -- as self-appointed gatekeepers to financial and employment opportunity. Their lack of innovation and propensity toward mistakes perpetuates injustices and denies opportunity to many, especially lower-income consumers and people of color. The second bill, the “Protecting Innocent Consumers Affected by a Shutdown Act,” will force the CRAs to lend a hand to the restoration of the financial lives of the government employees and contractors harmed by the recent extended shutdown. Since 1989, I have observed the arrogant attitude of the CRAs. They’ve always claimed that mistakes, let alone credit problems, aren’t their fault; they simply report what they are told. It is literally the Bart Simpson defense: “It’s not my fault.” They won’t change unless you make them. Passage of these two bills will make them change.

---

<sup>4</sup> In 1992, after Congressional consumer champions could not remove an amendment inserted in committee at the behest of the banks and CRAs, preempting all state laws under the FCRA, consideration of the Consumer Credit Reporting Reform Act of 1991, HR3596, was ended by a “House motion to rise” requested by consumer groups. See <https://www.congress.gov/bill/102nd-congress/house-bill/3596>

## **2. This Story Is About Consumers, Who Are Products, Not Customers, of the CRAs**

This story is not simply about three big CRAs (credit bureaus) named Equifax, Experian and Trans Union. It is also about numerous specialty credit bureaus and also about numerous emerging companies that don't know or don't want to admit their products are consumer credit reports regulated under the FCRA.

It is also about the responsibilities of the creditors that voluntarily "furnish" information to CRAs.<sup>5</sup> Why do they do this? The theory is simple. If more credit files are available about more consumers and contain more trade lines (accounts) about consumer history, then the consumer reporting database will be more valuable to users. Most of the creditor-furnishers of information to the CRAs are also customer-users of the CRAs. The business customers gain the benefit of a larger database; they also have responsibilities as users of credit reports.

Yet, mostly it is about the plight of **consumers** whose financial and other histories are the subjects of credit reports, which are bought and sold without our consent. **We are not their customers; we are their product.** Note that this has not stopped the CRAs from developing a lucrative, multi-billion dollar marketing channel of subscription-based credit monitoring and identity theft protection products designed to play to our fears of low credit scores or imposters stealing our name.<sup>6</sup>

In reality those credit scores are low because the CRAs haven't been forced to do a better job protecting our files from misuse or to keep them accurate or to respond to us properly when we dispute the mistakes. Imposters prevail because of flaws in the credit granting system and debacles such as the Equifax breach that make financial DNA freely available. Instead of carrying out their statutory duties, the CRAs have persisted in ignoring them while simultaneously aggressively hawking a variety of over-priced self-help products.

In 2017, the CFPB fined Equifax \$2.5 million; Transunion \$3 million and Experian \$3 million over deceptive marketing of credit monitoring products by offering deceptively marketing "educational" credit scoring products, not the scores actually used by lenders to make decisions. The CFPB also ordered Transunion to pay \$13.8 million and Equifax to pay \$3.8 million in consumer refunds for using bait and switch trial subscriptions.<sup>7</sup> If these products had the actual

<sup>5</sup> Furnishers did not have any duties until 1996 amendments. Duties to provide complete and accurate information are solely enforceable by regulators; private enforcement is available only when furnishers are notified of reinvestigation disputes (See FCRA Section 623, 15 USC 1681s-2).

<sup>6</sup> This lucrative channel includes identity theft protection and subscription credit scoring products. "The private research firm IBISWorld estimated that the U.S. market for identity theft services was about \$3 billion in 2015 and 2016." See page 5, "Identity Theft Protection Services," U.S. GAO, March 2017, available at <https://www.gao.gov/assets/690/683842.pdf>.

<sup>7</sup> These enforcement actions were carried out under the first confirmed CFPB director, Richard Cordray. News release, CFPB, "CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products," 3 Jan 2017, see <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/> and News Release, CFPB, "CFPB Fines Experian \$3 Million for Deceiving Consumers in Marketing Credit Scores," 23 March 2017, see <https://www.consumerfinance.gov/about-us/newsroom/cfpb-fines-experian-3-million-deceiving-consumers-marketing-credit-scores/>

value affixed to the price (\$19.99/month and up), they would be sold as stand-alone products that would jump off the shelves.

### **3. What triggered passage of the 1970 Fair Credit Reporting Act?**

In 1968 Representative Clement Zablocki (WI) offered an unsuccessful amendment to regulate credit reporting during consideration of the original Truth In Lending Act. Hearings were then held by the Senate and House by Sen. William Proxmire (WI) and Rep. Leonor Sullivan (MO). The complaints that triggered Congressional interest focused on a variety of deprivations by credit bureaus but a key driver of the hearings was complaints about the Retail Credit Company's abusive investigations of consumers applying for insurance policies. The Fair Credit Reporting Act was enacted in 1970 and in 1975, Retail Credit Company changed its name to Equifax.

While the original act restricted the sale of reports to limited purposes, provided certain rights for consumers and imposed responsibilities on credit bureaus and credit report users (but not yet on voluntary "furnishers of information"), some consumer advocates withdrew support when the final law included an industry-supported amendment providing qualified immunity from state defamation laws.

### **Early Consolidation Led to Mistake Patterns and Lack of Compliance That Continue Today; Sloppy Practices Also Lead to Identity Theft**

Following passage of the act and the acceleration of industrial computerization, local and state credit bureaus began a first major wave of consolidation that resulted in 5, then 3 national CRAs by the early 1990s. A series of early 1990s reports by U.S. PIRG, Consumer Union (now Consumer Reports) and certain non-aligned CRAs confirmed widespread complaints.<sup>8</sup> U.S. PIRG, through FOIA requests, found credit bureau complaints led all others to the FTC in the early 1990s.<sup>9</sup> The consolidation of databases written in different programming languages and

<sup>8</sup> James Williams of Consolidated Information Services, a New York area retail mortgage credit reporting agency, in 1991 analyzed 1500 reports from the three big bureaus and found errors in 43 percent of the files. It and other smaller resellers of consumer credit reports are regulated by the FCRA; they are also customers of the Big 3, which are also known as data repositories. Over time, the number of these resellers, which in the 1980s and 1990s had an important role in conducting manual underwriting (line-by-line human review of consumer credit reports) has dwindled and their business models have changed, under pressure from the CRAs. But they have produced at least one other study of accuracy. See, for example, Consumer Federation of America and the National Credit Reporting Association, "Credit Score Accuracy and Implications for Consumers," 17 Dec 2002, at [https://consumerfed.org/pdfs/121702CFA\\_NCRA\\_Credit\\_Score\\_Report\\_Final.pdf](https://consumerfed.org/pdfs/121702CFA_NCRA_Credit_Score_Report_Final.pdf). This detailed study of credit scores derived from over 500,000 consumer credit files also provides a useful history of other studies of credit reporting accuracy and a discussion of the migration of credit and, especially, mortgage decision-making from manual to automated underwriting.

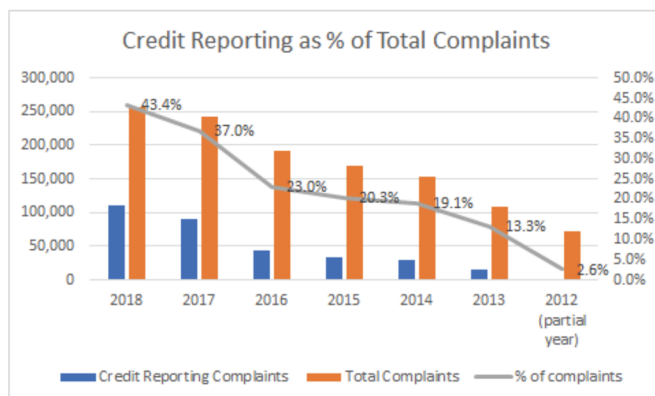
<sup>9</sup> See the following state PIRG reports: *Nightmare On Credit Street (Or How The Credit Bureau Ruined My Life): Case Studies Documenting Consumer Complaints and Recommendation For Amending the FCRA*, June 12, 1990; *Don't Call; Don't Write; We Don't Care*, 1991, which reviewed 156 consumer report complaints on file at the FTC and revealed that the average duration of complaints against a credit bureau was 22.5 weeks, or almost 6 months; and *Public Enemy #1 at the FTC*, "October 1993. Based on a Freedom of Information Act request, the 1993 report found that between 1990 and 1993, problems with credit bureaus was the leading cause of complaints to the FTC (30,901, 20.6%). *Public Enemy* also found

non-standard reporting formats – along with lax enforcement of the law – certainly contributed to the problems identified by the FTC, state attorneys general, Congress and consumer groups.

The mistakes and problems we found in the early 1990s continued. In the mid-1990s, we documented the rise of identity theft, which left more consumers struggling with the credit report dispute process.<sup>10</sup> ID theft was fueled by the easy availability of Social Security Numbers and a security flaw in the credit granting process. An identity thief doesn't need to obtain your credit report (which requires you to verify a lot of identifying information, try it). The thief simply applied for credit in your name, with your SSN and his/her address. The retailer or creditor, a trusted third party to the CRAs, obtains your credit report and issues credit in your name, to the imposter using your SSN, at the imposter's address.

In 2013, the Federal Trade Commission found that 26% of consumers had at least one mistake that "might affect their credit scores" in one of their credit reports and 5% of all consumers had "errors on one of their three major credit reports that could lead to them paying more for products such as auto loans and insurance."<sup>11</sup>

U.S. PIRG's regular reviews of the very important CFPB Public Consumer Complaint Database have most recently found the following, with 85% of all credit reporting complaints directed at Equifax, Experian and TransUnion:

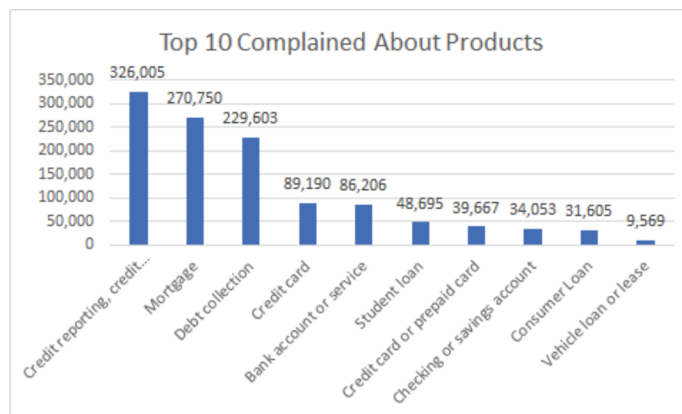


that 44% of complaints concerned mixed files, and that among those, 64% involved the mixing of data with total strangers. We have published additional reports on consumer reporting errors, disputes and complaints in 1998, 2004 and 2014.

<sup>10</sup> See CALPIRG and U.S. PIRG, "Identity Theft: The Consumer X-Files," 1996, and "Identity Theft II: Return to the Consumer X-Files" and CALPIRG and the Privacy Rights Clearinghouse, "Nowhere to Turn: Stories from Identity Theft Victims," 2000.

<sup>11</sup> Federal Trade Commission, "In FTC Study, Five Percent of Consumers Had Errors on Their Credit Reports That Could Result in Less Favorable Terms for Loans," 11 Feb 2013, see <https://www.ftc.gov/news-events/press-releases/2013/02/ftc-study-five-percent-consumers-had-errors-their-credit-reports>





The public CFPB Consumer Complaint Database is a critical tool for consumers, academics and other researchers and even competitors to make consumer financial markets work better.<sup>12</sup> Efforts by special interest groups to kill it must be rejected.<sup>13</sup>

#### **4. The Failures of the FTC To Bring the CRAs to Heel Over 40 Years**

The Federal Trade Commission fought the credit bureaus with one hand tied behind its back from 1970-2010. The FTC had no or little rulemaking authority under the FCRA nor did it have supervisory or examination authority—the right to look inside the black box of CRA operations at any time to determine compliance and stop problems before the problems became worse.

Since 1970, we are only aware of one public civil penalty imposed by the FTC against the three CRAs for violating the FCRA. In 2000, in an action called Operational Busy Signal, the 3 were fined a total of \$2.5 million for not having enough human staff to answer the complaint hotlines.<sup>14</sup> In 2007, under the FTC Act, not the FCRA, Experian subsidiaries were fined \$300,000 for violating a consent decree issued in 2005 for deceptive marketing of its credit report monitoring subscription products.

<sup>12</sup> Since 2013, U.S. PIRG has released more than a dozen reports analyzing complaints in the database, on subjects including credit reports, and on categories of consumers, including the targeting of servicemembers by financial predators. See <https://uspirg.org/page/usp/reports-cfpb-gets-results-consumers>

<sup>13</sup> Our June 2018 report, “Shining A Light on Consumer Problems: The Case for Public Access to the CFPB Complaint Database,” summarizes why the database must remain open. See <https://uspirg.org/reports/usp/shining-light-consumer-problems>

<sup>14</sup> In 2000, Experian and TransUnion were fined \$1 Million and Equifax \$500,000 for a total of \$2,500,000 in the FTC’s “Operation Busy Signal,” for failing to comply with a 1996 amendment to have adequate humans on hand to answer complaint calls.

Creation of the new Consumer Financial Protection Bureau, established by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, largely remedied these deficiencies. The CFPB was given full rulemaking over 19 different consumer laws, including the FCRA.<sup>15</sup> The CFPB also has other authorities that the FTC lacks, including the right to impose penalties at any time<sup>16</sup> and supervisory or examination authority<sup>17</sup>—the right to look inside the black box of covered firms at any time to determine compliance and stop problems before the problems became worse.

The CFPB has exercised robust research,<sup>18</sup> examination and supervisory authority over the consumer reporting markets.<sup>19</sup> Yet, in one curious exception, with relevance to the Equifax breach, authority over CRA data security was retained by the FTC in Section 1031 of the Dodd-Frank Act. Title V of the Gramm-Leach-Bliley Act of 1999 had given the FTC authority to write rules establishing data security responsibilities for non-bank financial firms, including CRAs. Its data security rule is known as the “Safeguards Rule.”<sup>20</sup> While the CFPB is reportedly pursuing an Equifax investigation and likely can defend its data security actions under its other authorities, it makes sense to transfer GLBA Title V authority to the CFPB, as recommended by the National Consumer Law Center in recent testimony before the committee.<sup>21</sup>

<sup>15</sup> The FTC retains joint authority over the FCRA, in addition, it retained a number of its own staff expert in the FCRA; annually the two agencies sign a Memorandum of Understanding concerning their shared FCRA duties.

<sup>16</sup> Although FTC can impose penalties for any violation of the FCRA or the Fair Debt Collection Practices Act, it can only impose civil penalties under either title core authority under the FTC Act or its GLBA requirements after a firm is found to be in violation of an FTC-imposed consent decree.

<sup>17</sup> Congress gave the CFPB supervisory authority over banks > \$10 Billion Dollars in asset size and over payday lenders, non-bank mortgage companies and private student lenders of any size. It also gave the Bureau, under Section 1024 of the Dodd-Frank Act, authority to write rules granting itself authority to supervise larger participants in other important financial markets. It has used the authority several times; notably, its first larger participant rule, in 2012, was over the consumer reporting markets. <https://www.federalregister.gov/documents/2012/07/20/2012-17603/defining-larger-participants-of-the-consumer-reporting-market>

<sup>18</sup> See “Key Dimensions and Processes in the U.S. Credit Reporting System: A review of how the nation’s largest credit bureaus manage consumer data,” December 2012, <https://www.consumerfinance.gov/data-research/research-reports/key-dimensions-and-processes-in-the-u-s-credit-reporting-system/>

<sup>19</sup> See “Supervisory Highlights: Consumer Reporting Special Edition,” 2 March 2017 <https://www.consumerfinance.gov/data-research/research-reports/supervisory-highlights-consumer-reporting-special-edition/>

<sup>20</sup> See <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule>

<sup>21</sup> See page 8, Testimony of Chi Chi Wu, National Consumer Law Center, House Financial Services Committee “Continuation of Hearing Examining the Equifax Breach,” 25 October 2017, <https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=400866>



### **5. Equifax Showed Gross Indifference to its Responsibilities to Protect Consumer Information; Its Data Breach Response Made Things Worse**

Several Congressional committees have held hearings and/or issued staff reports detailing the Equifax breach. U.S. PIRG's own September 2018 report, "Equifax Breach One Year Later," summarized the following major problems:<sup>22</sup>

Had Equifax not been so careless, the breach may never have happened. Four months before the hacking, Equifax could have fixed a known security vulnerability in the widely-available and used Apache Struts open-source platform. Innumerable warnings from government security agencies and private experts were not acted on.

As explained in our report, the company also botched its response by:

- Delaying public notification for at least six weeks
- Setting up an online search tool that provided faulty results to those who used it about whether they were affected by the breach
- Initially understaffing its call center
- Initially including arbitration language that forced consumers to sign away their rights to a day in court
- Directing consumers to a fake website
- Failing to provide consumers full protection from new account identity theft -- which it still hasn't done. (See Appendix A for a summary of Equifax's offerings to consumers in response to the breach and how they fall short of protecting consumers.)

Despite all the outrage and media attention last year, Congress has done little except make security freezes free, and even then, done so in a manner favorable to Equifax and the other CRAs, by preempting the right of states to enact stronger freeze protections going forward. Of course, the idea of the freeze didn't come from Congress, it came from 50 state freeze laws passed between 2003 and 2018. The idea of the free freeze also was jump-started by several free freeze amendments to existing state laws passed after the 2017 Equifax breach but before Congress passed S2155 in May 2018. That law created several minor consumer protections—but both the preemptive free freeze right and a military credit monitoring “right without a remedy” if monitoring was not provided were imperfect efforts. The comprehensive Waters CCRRA reform will cure both these problems. Congress should never preempt the states, especially at the behest of powerful special interests.

Also, critically important, Equifax has neither been held accountable nor paid a price for its breach. Further, this sensitive information, including Social Security numbers and birth dates, is still out there, with the potential to wreak havoc for the majority of consumers in perpetuity.

### **6. It Is Critical to Pass the Two Bills Before the Committee Today**

Finally, we offer our strong support to the two discussion drafts from Chairwoman Waters and her co-sponsors before the committee today. The first, the Comprehensive Consumer Credit

<sup>22</sup> Mike Litt, U.S. PIRG, “Equifax Breach: One Year Later: How to Protect Yourself Against ID Theft & Hold Equifax Accountable,” 6 Sept 2018, available at <https://uspirg.org/reports/usp/equifax-breach-one-year-later>

Reporting Reform Act (CCRRA) of 2019, is a new version of the Chairwoman's longstanding effort to correct flaws in the consumer reporting system. It is a broad and thoughtful response to the problems posed to all consumers by the failure of the consumer reporting system, dominated by its Big 3 members as self-appointed gatekeepers to financial and employment opportunity. These firms have demonstrated for years that they lack the key incentives to do their jobs. Their failures perpetuate injustices that raise costs for nearly everyone and deny opportunity to many.

The second bill, the "Protecting Innocent Consumers Affected by a Shutdown Act," will force the CRAs to lend a hand to the restoration of the financial lives of the government employees and contractors harmed by the recent extended shutdown.

Since 1989, I have observed the bad attitude of the CRAs. They've always claimed that mistakes, let alone credit problems, aren't their fault; no, they claim "we simply report what we are told and if it is wrong, or negative, so what." They won't change unless you make them. The shutdown bill will make them take action to help people harmed through no fault of their own. The CCRRA addresses endemic problems in the consumer reporting system.

#### **Title I of CCRRA: New Right of Appeal Critical to "Fixing the Dispute Process"**

I will never forget the plea to the FTC by one of the consumers highlighted in U.S. PIRG's first report on credit bureau errors and failure to fix them. In 1990, the consumer asked: "It says 'Item Remains, Confirmed By Source.' What is this source!?" A review of several narratives in the CFPB public consumer complaint database finds similar unanswered complaints from consumers continue today:

"Experian states that the information remains..." [or] "Equifax completed the investigation yet this item still remains on my Equifax Credit Report..." [or] "According to TransUnion's updated credit file on XX/XX/2017 ( # XXXX ), XXXX # XXXX ... should be removed XX/XX/2017. As of XX/XX/2017, this item remains..." [or] "their responsibility must consist of something more than merely parroting information received from other sources..." [or] "I have asked Experian to provide the name of the data furnisher or third party source who verified this information so that I can contact them directly. Experian refuses to provide this information..." [or] "I have disputed this account several times online and in writing with no resolution. This account still remains on my credit report..."

So, the dispute system, despite efforts in 1996 and 2003 to fix it, is still broken. Title I of the CCRRA makes significant improvements. Most notably, for the first time, it establishes a right to appeal disputes. Title I also includes new matching procedures and other requirements to prevent disputed information from being routinely reinserted into consumer reports. Until now, greater weight has been placed on the opinion of "the source" furnisher than the consumer and less weight has been placed on whether an actual reinvestigation ever occurred, or whether the furnisher and CRA computers simply agreed that they both contained the same data, even if it was wrong.

### **Title II of CCRRA Limits the Use of Consumer Reports for Most Employment Decisions**

Several states, including California, Colorado, Maryland and Oregon, and cities such as Chicago and New York have restricted the use of consumer reports for employment decisions. Further, the industry has admitted in testimony that it cannot show a relationship between a consumer's credit report and job performance.

Further, should any consumer be denied employment opportunity in a difficult economy due to a disputed item, or even an actual late payment, on a credit card?<sup>23</sup> The problem is harshest on persons of color and lower income consumers with "thinner" credit reports. Historically, their credit opportunities have not been extended from the national firms that dominate the credit system. Should their job opportunities be similarly diminished by their credit reports?

### **Title III of CCRRA Improves Rights of Victims of Private Student Loan Borrowers**

The title provides new protections for victims, including servicemembers and others, of unfair private student loan practices.

### **Title IV of CCRRA Makes a Variety of Changes to Rebalance the Reporting of Adverse Items**

Credit scoring models prioritize the value of recent trade line information over much older information. Begrudgingly, under order by enforcement actions, the CRAs have also reduced the impact of non-predictive data, such as medical debt, and removed public records known to be full of misinformation. Yet, in general the CRAs have long resisted any changes to the types of information that they can collect or report or how long they can report it, even if it is now known to be non-predictive.

Title IV makes important changes to make reports more accurate and predictive. It shortens the reporting of certain bankruptcies from 10 to 7 years, eliminates reporting of certain public records and reduces the reporting of credit trade lines from 7 to 4 years, among other changes. It greatly reduces the impact of medical debt items, which are often mistaken due to bills that should be the responsibility of slow-pay insurance companies but are sent to collection under the consumer's name. Further, medical debt is the result of getting sick, or laid off, or losing insurance coverage, not due to a propensity toward "spending sprees." Both leading credit scoring models, FICO and VantageScore, a joint venture of the Big 3 CRAs, have already reduced or eliminated reliance on medical debt items.

Title IV also provides protection to victims of for-profit schools and other abusive practices.

### **Title V of CCRRA Establishes Oversight of Credit Scoring Models and the Use of Non-Traditional Data**

Title V gives the Consumer Bureau clear authority to monitor and oversee the validity of credit scoring models to ensure that the often-opaque algorithms are accurate and predictive and do not

<sup>23</sup> See testimony of Chi Chi Wu, National Consumer Law Center, at a "Legislative Hearing on HR3149, the Equal Credit For All Act," Subcommittee on Financial Services and Consumer Credit, 23 Sept 2010, <http://archives-financialservices.house.gov/Hearings/hearingDetails.aspx?NewsID=1355>

introduce scoring factors that could violate the civil rights or fair lending laws. Further, Title V requires a Consumer Bureau study of the use of non-traditional data in consumer reporting. Alternative data is a shiny new toy you'll hear a lot about, but could have negative or unintended consequences, especially for some of the populations its proponents claim that it will assist.

**Title VI of CCRRA Provides for Free Annual Credit Scores and Improves Requirements on Consumer Report User Firms to Promote Consumer Understanding of the Use of Reports and Scores**

In the early 1990s the FTC proposed an interpretation that credit scores were, by definition, part of consumer credit reports that should be included in credit report disclosures<sup>24</sup> to consumers. Under an industry full-court press, it immediately reneged on this consumer-backed idea.

In 2000, following a joint campaign by realtors and consumer groups, California prohibited clauses in CRA contracts with users such as real estate agents that prevented them from showing credit scores to consumers. Since then, the veil over credit scores has gradually lifted. The CRAs have long-sought to monetize their disclosure, unfortunately also through deceptive marketing of “educational” scores, not the scores actually used by creditors.<sup>25</sup> It is past time to provide scores for free as part of the annual free report disclosure first required nationwide by the 2003 FACT Act. Section 604 of the CCRRA provides free credit scores in this and other circumstances.

Title VI also requires various users to provide consumers with additional information to improve their understanding of the consumer reporting system.

**Title VII of CCRRA Bans Misleading and Unfair Consumer Reporting Practices**

Even though we are not their customers, only their product, nothing has stopped the CRAs from developing a lucrative, multi-billion-dollar marketing channel of subscription-based consumer credit monitoring and identity theft protection products designed to play to our fears of low credit scores or imposters stealing our name.

Our credit scores are low because the CRAs haven't been forced to do a better job protecting our files from misuse or to keep them accurate or to respond to us properly when we dispute the mistakes. Instead of carrying out these statutory duties, the CRAs have persisted in aggressively hawking a variety of over-priced self-help products, often in an unfair or deceptive way.<sup>26</sup> Title

---

<sup>24</sup> The FTC did not have any rulemaking authority under the FCRA until limited authorities were granted in the 2003 FACT Act. In previous years, its views were described in often-amended “FCRA Interpretations” and through staff opinion letters.

<sup>25</sup> The CFPB used director Richard Cordray's bully pulpit very effectively to nudge more banks and credit unions to greatly expand the availability of free credit scores. Its most recent list is available: Skyricki, Irene, “A new list identifies more ways to access credit scores—for free,” CFPB, 16 May 2018, at <https://www.consumerfinance.gov/about-us/blog/new-list-identifies-more-ways-access-credit-scores-free/>

<sup>26</sup> For deceptive marketing of subscription products by CRAs, see news release, CFPB, “CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products,” 3 Jan 2017, at <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/> and News Release, CFPB, “CFPB Fines Experian \$3 Million for Deceiving Consumers in Marketing Credit Scores,” 23

VII would provide a variety of new protections against unfair and deceptive marketing of these products. Low-value versions of these products are often provided free after a data breach but consumers face a barrage of online and televised ads extolling the supposed virtues of upgrading to a \$19.99/month, or even higher-priced, products. Section 703 gives the Consumer Bureau authority to restrict the prices of the subscription products.

Title VII provides additional protections to consumers with limited English proficiency and mandates by law that shopping around, for example, for a good deal on a new car, is not treated in credit scores as multiple applications for credit with multiple “dings” to a credit score. Further Section 707 establishes, for the first time, national registration of national and specialty CRAs to make it easier for the Consumer Bureau, FTC and consumers to hold them accountable.

#### **Highlights of Title VIII of CCRA, Which Provides Additional Consumer Protections**

The CRAs have long-imposed barriers on consumers fighting identity theft. Section 801 makes clear that there are a variety of ways a consumer can file a lawful identity theft affidavit, even if their local police do not take identity theft complaints. Most don’t.

Section 802 makes improvements to the rights of protected or incapacitated consumers.

Section 803 improves statutory fraud alert rights for both consumers and active duty military personnel.

Section 804 corrects a CRA-driven provision in 2018 amendments that established a free national credit freeze right, but preempted states from providing additional, stronger protections. Section 808 corrects a separate 2018 amendment that provided servicemembers with free credit monitoring, but did not give them a remedy if the services were not provided.<sup>27</sup>

Title IX makes certain other amendments to ensure that the CRAs and other firms act in the public interest and under the law and requires the Consumer Bureau to complete rulemaking under the CCRRA within two years of passage.

#### **6. Conclusion**

This testimony and the attached timeline make an effort to describe how consumer reporting agencies have no incentives to sell accurate credit reports, so they do not. We also concur with the detailed testimony of my consumer and civil rights colleagues on the panel today, as well as the statements for the record submitted by a number of other consumer and civil rights advocates.

To protect consumers and ensure that markets work fairly, a combination of strong federal laws enforced by strong federal agencies must be accompanied by the right of states to respond more quickly to new threats in the marketplace. Further, full enforcement rights by state Attorneys

---

March 2017, at <https://www.consumerfinance.gov/about-us/newsroom/cfpb-fines-experian-3-million-deceiving-consumers-marketing-credit-scores/>

<sup>27</sup> The provisions were included in S2155, a deregulatory proposal which became law as the Economic Growth, Regulatory Relief, and Consumer Protection Act (Public Law 115–174).

General and local officials and strong private rights of action so that consumer protection attorneys can act as private attorneys general are also needed. The message is clear. Congress cannot solve every problem. Federal agencies cannot go it alone.

Going forward, we also look forward to working with the committee on newer and emerging problems of consumer protection, privacy and digital rights in the financial marketplace. For example, a large class of nearly unregulated data brokers sells products that are virtually identical to consumer credit reports, but not sold for “credit, insurance or employment purposes,” so remain outside the protections of the FCRA. So-called lead generators sell lists of consumers, including to predatory lenders, derived from tracking their Internet activities. Pre-approved marketing decisions are being made, in real time, based on unregulated “e-scores” and look-alike consumers. Since the reports are not about a particular consumer, the firms contend their products are not regulated consumer reports.

As we point out on our “Digital Data and Consumer Protection Page:<sup>28</sup>”

“American consumers face new challenges and opportunities to their financial security as our economy is transformed by the convergence of digital media with “Big Data” technologies. Our use of mobile phones, social media, “apps,” and other online tools have created new ways for us to spend, save and borrow money. Powerful forces are at work, however, that can undermine a consumer’s ability to make the best choices and may place those already financially at risk even more vulnerable. The digital data-driven economy continually gathers vast amounts of information on individuals, online and offline, which is used to create a “profile” about our spending habits, behavior and our geo-location. These profiles can be “scored”—an invisible measure known only to the marketer and data brokers—that can determine whether we are offered high interest credit cards, payday and for-profit college loans and even what we may pay at retail and grocery stores. The uses of the information can be positive or, absent any regulation or meaningful protections, lead to discrimination, price manipulation or denied opportunity.”

Thank you again for the opportunity to provide our views to the committee today. I look forward to your questions.

#### **Appendix: Timeline of Significant Credit Reporting Events and Policymaker Responses**

---

<sup>28</sup> See <https://uspirgedfund.org/issues/usf/digital-data-and-consumer-protection-ensuring-fair-and-equitable-financial-marketplace>

QUICK TIMELINE OF SELECTED CREDIT BUREAU (or CRA) EVENTS 1960s-TODAY		
Date	Problem/Policy	What Was the Problem; What was Response?
Late '60s	<b>CRA Problem</b>	Complaints grow about Retail Credit Corporation (now Equifax) insurance consumer report scandal
1970	Federal Response	<b>Congress holds hearings on scandal; enacts Fair Credit Reporting Act to regulate companies selling consumer reports (called credit bureaus or CRAs)</b>
1980s	<b>CRA Problem</b>	First wave of consolidation of local/regional credit bureaus results in increase in errors in consumer credit reports
80s-early '90s	Both State/Federal Response	Responding to errors, investigations by state attorneys general and FTC result in CRAs brought under consent decrees, no fines
		-- TRW (now Experian) signs multi-state and FTC consent order in 1991
		-- Equifax signs consent orders with states (1992) and FTC (1996)
		-- Trans Union signs consent orders with states in 1992 and FTC in 1994
1989	Federal Response	House Banking Committee (now FSC) holds first hearings in years on credit bureau errors
1991	<b>CRA Problem</b>	TRW (now Experian) incorrectly reports all citizens (3,000) of Norwich, VT area had failed to pay their taxes.
1992 - today	<b>CRA Problem</b>	By early 1990s, consolidations result in powerful gatekeeper "Big 3" national CRAs which now continue to acquire specialty competitors
1992	<b>CRA Problem</b>	<b>Sponsors remove FCRA reform, HR3596, from floor action due to sweeping preemption provision demanded by banks/credit bureaus</b>
Early 1990s	CRA Problem & Bad Policy Response	Use of non-transparent credit scores grows, FTC proposes FCRA interpretation that scores are part of credit reports; under industry pressure, reverses itself.
1992-1996	State Response	<b>States led by Vermont and California enact comprehensive credit report reforms; 7 states provide annual free credit reports (VT, then CO, GA, MA, ME, MD, and NJ)</b>
1994-today	<b>CRA Problem</b>	Rise of instant credit, easy availability of SSNs, other financial DNA, fuel rise of identity theft
1995-present	<b>CRA Problem</b>	<b>Instead of improving compliance, CRAs respond to threat of errors/identity thieves by intensifying scare marketing of credit monitoring add-on products to consumers --now fueling a \$3 Billion/year marketing channel per GAO</b>
1996	Federal Response	<b>Congress finally passes Consumer Credit Reform Act (largely 1992's HR3596), imposes first duties on furnishers [creditors and debt collectors that provide information to credit bureaus] among other reforms. Limited preemption, primarily for new furnisher (bank) duties, to sunset after 8 years.</b>
1998	Federal Response	Congress criminalizes identity theft, bureaus can now claim ID theft not our fault, "it's bad guys."



QUICK TIMELINE OF SELECTED CREDIT BUREAU (or CRA) EVENTS 1960s-TODAY		
Date	Problem/Policy	What Was the Problem; What was Response?
2000	Federal Response	Big 3 CRAs fined total of \$2.5M (Experian \$1M; Equifax \$500k; TransUnion \$1M) in Operation Busy Signal for failing to comply w/ 1996 amendment to have adequate humans to answer complaint calls
1998-2000	State Response	California realtors join consumer groups to win right for consumers to see their credit scores, previously prohibited by CRA contracts with user companies
2002	State Response	California enacts first data breach notice law
2003	State Response	California develops/enacts credit freeze protection right to deter identity thieves
2003	Federal Response	Congress passes FACT Act; limited bank preemption made permanent; annual free credit reports (but not free scores) included. Few identity theft fixes.
2003-2018	State Response	Following PIRG/Consumers Union model law, 50 states enact credit freeze and data breach notice laws to supplement omissions in FACTA.
2003	Consumer Action	Consumer protection attorney wins first case against a creditor-furnisher for failing to comply with FCRA in dispute investigation
2005	CRA Problem	Equifax spinoff ChoicePoint fined record \$25M by FTC for selling credit reports to identity thieves
2005-2007	CRA Problem	Experian subsidiaries deceptively market subscription-based credit monitoring products by intentionally confusing them w/ free credit report by law
2005-2007	Federal Response	FTC places Experian under consent order in 2005 for deceptive marketing of subscription products, orders \$300k penalty in 2007 for violating 2005 order under FTC Act
1970-2010	CRA Problem	FTC's lack of tools to enforce FCRA leaves consumers at risk of credit and job denial and identity theft as credit bureaus run amuck
2010	Federal Response	Dodd-Frank Act gives CFPB primary authority over FCRA and new tools to regulate/supervise/investigate/enforce violations of the FCRA
2012	Federal Response	In CFPB's first establishment of a "larger participant rule," agency begins examinations (supervision) of large Consumer Reporting Agencies
2012	Federal Response	Major FTC study finds 26% of consumers have errors on at least 1 report; 5% of consumers have a serious error that could cause denial of credit or higher costs for credit
2013	Federal Response	CFPB supervision results in CRAs sharing full consumer complaint files instead of 2-digit summary codes, w/ furnisher creditors in disputes, which advocates contend 1996 amendments had required for over 15 years.
1995-present	CRA Problem	Instead of improving compliance, CRAs respond to sloppy mistake-ridden reports/growth of identity theft by intensifying scare marketing of credit monitoring add-on products to consumers -- now fueling a \$3 Billion marketing channel, per GAO, even though consumers are their products, not their customers



QUICK TIMELINE OF SELECTED CREDIT BUREAU (or CRA) EVENTS 1960s-TODAY		
Date	Problem/Policy	What Was the Problem; What was Response?
2017	Federal Response	CFPB fines Equifax \$2.5 million; Transunion \$3 million and Experian \$3 million over deceptive marketing of credit monitoring products by offering "FAKO," not FICO-like, credit scoring products. Also orders Transunion to pay \$13.8 million and Equifax to pay \$3.8 million in consumer refunds for using bait & switch trial subscriptions
2017	Consumer Action	Consumer protection attorneys win \$60 Million jury verdict against TransUnion for falsely labeling 8,000 consumers as terrorists or drug traffickers.
2012-2017	Federal Response	CFPB releases "Key Dimensions report" and several "Supervisory Highlights" reports that document deficiencies in the Big Three CRAs' dispute systems, confirming findings in NCLC's 2009 Automated Injustice report
2014-2017	Both State/Federal Response	CFPB supervisory actions and a 31-state Attorney General settlement eliminate tax liens and civil judgements (often posted with inaccurate identifying information) from reports, raising credit scores for 12 million; and reduce the negative impact of medical debt on scores.
2015	CRA Problem	Data breach at Experian involving database used for T-Mobile customers affects 15 million consumers
2017	CRA Problem	Equifax breach: sloppy data security makes SSNs, other sensitive information for 148 million consumers available to outsiders
2019	Federal Response To Breaches	Still Waiting...
2019	Federal Response	Chairwoman Maxine Waters of House FSC Holds Important Hearing To Review Equifax Breach Response and Discuss Necessary Improvements To FCRA
Thanks to Chi Chi Wu of National Consumer Law Center for providing ideas.		
U.S. PIRG is responsible for any inaccuracies.		



The App Association

Jessica Herron  
Legislative Clerk  
Subcommittee on Innovation, Data, and Commerce  
House Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, District of Columbia 20515

Re: Morgan Reed's Responses to Additional Questions for the Record

Dear Ms. Herron,

Thank you for inviting me to testify on behalf of ACT | The App Association on April 27, 2023, at the hearing, "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information."

Pursuant to the Committee on Energy and Commerce's Rules, I am attaching my answers to additional questions for the record in the required format.

Please let me know if you have any additional questions or if it would help for us to meet with Subcommittee staff as you continue your work on privacy legislation.

Sincerely,

A handwritten signature in black ink that reads "Morgan Reed". The signature is fluid and cursive, with the first name "Morgan" and last name "Reed" clearly distinguishable.

Morgan Reed  
President  
ACT | The App Association

The Honorable Kelly Armstrong

1. **The Federal Trade Commission (FTC) advance notice of proposed rulemaking (ANPR) on “Trade Regulation Rule on Commercial Surveillance and Data Security” refers to “different kinds of consumers” and appears to consider employees as a type of consumer. The statement of Chair Khan regarding the ANPR also references “...tracking, collection, and analysis of consumer data in the workplace...”, which seems to be a reference to employee data. The dissenting statement of then-Commissioner Noah Phillips disagrees that the Federal Trade Commission Act confers jurisdiction on the FTC to “regulate any aspect of the employer-employee relationship that happens to involve data.” It is evident that the employer-employee relationship is fundamentally different compared to a business-consumer relationship. An employer must process employee data for several purposes, including compliance with state and federal labor laws and other purposes related to professional activities. How would FTC action to regulate employee data impose challenges on the employer-employee relationship and existing laws governing that relationship?**

I agree with the premise that the employer-employee relationship is fundamentally different compared to a business-consumer relationship. In our advocacy on privacy, the App Association has consistently urged lawmakers to ensure that however they decide to establish prohibitions on net harmful privacy conduct, those rules must respect the context of the business-consumer relationship. Employees’ relationships with their employer are different enough from the business-consumer context that applying the same rules to both scenarios would result in awkward and ultimately harmful outcomes that policymakers would have to clean up later down the road. The contractual relationships at issue in these scenarios necessarily lead to differing privacy considerations. Whereas consumers pay companies for a given product or service (either monetarily or by allowing access to data about themselves), businesses pay employees for services in furtherance of the employer’s production goals. Respect for context necessitates separate legislative—and regulatory—processes to consider the privacy issues that flow from these relationships.

The American Data Privacy and Protection Act (ADPPA) appropriately excludes “employee data” from the scope of “covered data.” Likewise, the Federal Trade Commission (FTC) shouldn’t seek to regulate privacy and security practices involving employee data under the same regime as consumer data. For example, mandating that employers respond to employee requests for access, deletion, or correction of data about themselves as if they were consumers of the company’s products or services creates several obvious problems. An employee might disagree with their supervisor’s characterizations of their performance and giving them a federally enforceable right to access any of their supervisor’s communications about them or correct any of that information would obviously have a dramatically negative effect on the ability for businesses to operate. Although the FTC’s Advance Notice of Proposed Rulemaking (ANPR) does not specifically ask questions about imposing requirements to respond to such consumer requests, any privacy framework policymakers ultimately pursue will likely include such requirements. Employers may also need to surveil employee activity—for example, to ensure safety or make timely adjustments to supply or staffing—in ways that would be inappropriate or at least communicated or conducted differently in the consumer-business context.

**The Honorable Russ Fulcher**

- 1. Does the ADPPA provide better and clearer guardrails on the use of data to allow for ensuring companies can engage in identifying for fraud protection, contractual issues, and yet, provide avenues for these same companies to work with their partners by sharing user information?**

Yes. Section 102 of ADPPA, which limits the data minimization principles in Section 101, appropriately allows for collection, processing, and transfer specifically for “fraud and identity fraud detection and prevention,” and contractual issues.

- 2. I want to understand better data processing requirements of the ADPPA and again how it might differ from the GDPR. This is due to many B2B companies (like technology platforms) that work with application partners or other fulfillment partners. How does the service provider relationship with your companies work currently within the sectoral laws? Or is this not an issue?**

There are lessons to be learned from how sectoral laws and the General Data Protection Regulation (GDPR) deal with the “controller” / “service provider” relationship. In general, the structure contemplated in the Health Insurance Portability and Accountability Act (HIPAA) appropriately delineates responsibilities between “controllers” (covered entities (CEs) under HIPAA) and “service providers” (business associates (BAs) under HIPAA). Under HIPAA, CEs are responsible for defining the scope of processing, collection, and transfer activities and communicating directly with patients about how they collect, process, and transfer protected health information. BAs may only process PHI provided to them through a CE via the contractual relationship they have with the CE and the contract defines the scope of what they are allowed to do with respect to that PHI. It is via that contract that HIPAA’s requirements apply to BAs. This is a logical construct for privacy, and it works similarly in GDPR. Many of my member companies have operations that put them under a BA agreement and operations that put them under the FTC Act. Likewise, I have member companies that are “controllers” under GDPR for some of their activities, but “service providers” for some of their other projects. Although the arrangements are complex, especially for small companies, having obligations flow via contracts through “controllers” to “service providers” is a better reflection of reality than making no distinction between those two categories.

- 3. Is there a worry over the lack of certainty for businesses in not having clarity over what obligations they will have to comply with when it comes to information collected from children that may not be protected under FERPA? Mr. Reed, how do your businesses view these challenges?**

Yes, the legal landscape applicable to collection, processing, and transfer of children’s data is complicated, whether the Family Educational Rights and Privacy Act (FERPA) applies or not. While the FTC has sought to clarify how FERPA and the FTC Act fit together, it is inevitable that the obligations that apply to education tech companies are ambiguous. In general, my member companies that provide education tools subject to FERPA pay closest attention to the

Children's Online Privacy Protection Act (COPPA) with respect to any of their activities that fall outside the scope of FERPA.

COPPA does operate a little differently from FERPA since FERPA regulates school districts (as opposed to businesses and their relationships with consumers). For example, COPPA's requirement for companies to obtain verifiable parental consent (VPC) prior to collecting PII from children does not apply "to the extent permitted under other provisions of law," (presumably, including FERPA's provisions). This could lead to the two regimes applying slightly unevenly or confusingly, even though there might be good reasons for their overlapping structure, but the FTC has addressed the issue. Under FERPA, schools need not obtain parental consent for disclosing children's education records to educational apps on contract with the school. The FTC has clarified in a frequently asked questions (FAQ) section that an education technology company may rely on "consent obtained from the school under COPPA instead of the parent," when such collection is for the "use and benefit of the school and for no other commercial purpose." Conversely, if the same children (if they are 12 or younger) sought to use the same educational apps outside the school context, the app must obtain VPC directly from those children's parents. Thus, while the edges around sector-specific privacy laws may seem less regulated, in this case, more regulatory privacy barriers arguably exist under the FTC framework than under the sector-specific law.

Ultimately, the takeaway for this Committee is that as it contemplates updates to children's privacy as part of ADPPA, there should be at least some focus on the burdens associated with VPC. As FTC Commissioners have pointed out, updates to privacy laws should avoid placing the burden on consumers wherever possible and instead place the burden of compliance on companies. VPC is an example of a requirement that places an inordinate burden on parents since it requires them to take seriously time-consuming steps to verify their identities with each and every service with which a child under 13 may interact. As a parent myself, I know that this is not a realistic burden to place on people as they seek to access educational services for their kids. And yet the current statute does not enable the market to provide VPC solutions in a convenient, organized way. It is often said that the notice-and-consent regime has failed because it doesn't fit real-world interactions between consumers and businesses. The same is true for VPC. A consumer privacy law can only ameliorate conditions for consumers to the extent it reflects reality and respects the ways consumers want to interact with and access digital goods and services.



May 27, 2023

Jessica Herron  
Legislative Clerk  
Subcommittee on Innovation, Data, and Commerce  
House Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515-6115

Re: Donald Codling's Responses to Additional Questions for the Record

Dear Ms. Herron:

I want to thank the Subcommittee for inviting me to appear before it on April 27, 2023, at the Innovation, Data, and Commerce hearing entitled, "Addressing America's Data Privacy Shortfalls: How A National Standard Fills Gaps To Protect Americans' Personal Information."

Pursuant to the Rules of the Committee on Energy and Commerce, I am attaching my answers to additional questions for the record, in the required format.

Thank you again for your help, and please let me know if you have any questions.

Sincerely,

A handwritten signature in dark ink that reads "Donald R. Codling". The signature is written in a cursive style with a large, stylized 'D' and 'C'.

Donald Codling  
Rego Senior Policy Advisor

**Attachment — Additional Questions for the Record**

**The Honorable Kelly Armstrong**

1. The Federal Trade Commission (FTC) advance notice of proposed rulemaking (ANPR) on “Trade Regulation Rule on Commercial Surveillance and Data Security” refers to “different kinds of consumers” and appears to consider employees as a type of consumer. The statement of Chair Khan regarding the ANPR also references “...tracking, collection, and analysis of consumer data in the workplace...”, which seems to be a reference to employee data. The dissenting statement of then-Commissioner Noah Phillips disagrees that the Federal Trade Commission Act confers jurisdiction on the FTC to “regulate any aspect of the employer-employee relationship that happens to involve data.” It is evident that the employer-employee relationship is fundamentally different compared to a business-consumer relationship. An employer must process employee data for several purposes, including compliance with state and federal labor laws and other purposes related to professional activities. How would FTC action to regulate employee data impose challenges on the employer-employee relationship and existing laws governing that relationship?
- A. Thank you for your question. However, we do not possess the necessary subject matter expertise and thus are unable to provide a view to answer this specific question.



May 25, 2023

Jessica Herron  
Legislative Clerk  
Subcommittee on Innovation, Data, and Commerce  
U.S. House of Representatives Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515

Dear Ms. Herron,

I want to thank the Subcommittee for including Salesforce expertise and perspective in its April 27, 2023 hearing entitled "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information". We hope that Members and staff found the hearing informative and helpful as they continue their work developing a national privacy standard. Please let us know if Salesforce can be of service in the future.

Pursuant to the Rules of the Committee, please find responses to questions for the record attached.

Sincerely,

Edward Britan  
Head of Global Privacy  
Salesforce

1801 K Street NW, Floor 4  
Washington, District of  
Columbia 20006  
Salesforce, Inc.  
📧 @salesforce





**Questions for the Record**

**The Honorable Kelly Armstrong**

The Federal Trade Commission (FTC) advance notice of proposed rulemaking (ANPR) on “Trade Regulation Rule on Commercial Surveillance and Data Security” refers to “different kinds of consumers” and appears to consider employees as a type of consumer. The statement of Chair Khan regarding the ANPR also references “...tracking, collection, and analysis of consumer data in the workplace...”, which seems to be a reference to employee data. The dissenting statement of then-Commissioner Noah Phillips disagrees that the Federal Trade Commission Act confers jurisdiction on the FTC to “regulate any aspect of the employer-employee relationship that happens to involve data.” It is evident that the employer-employee relationship is fundamentally different compared to a business-consumer relationship. An employer must process employee data for several purposes, including compliance with state and federal labor laws and other purposes related to professional activities. How would FTC action to regulate employee data impose challenges on the employer-employee relationship and existing laws governing that relationship?

In the U.S. we have a consumer-oriented privacy culture. The FTC should focus its ANPR on “Commercial Surveillance and Data Security” on protections for consumers. This will enable the ANPR and future rules stemming from it to gain more traction and be more effectively implemented.

There is a separate, well-developed field of employment law with which organizations must comply to protect employees. Salesforce believes that new employee-specific laws should be introduced to protect employee privacy. These laws could be enforced by the FTC with clear statutory guardrails to ensure that enforcement does not conflict with the existing employment legal structure.

Protecting employees in an ANPR primarily aimed at protecting consumers seems like a forced fit. Further, it would have unintended consequences in the employment context where obligations for consumer-facing companies and/or rights intended for consumers may come into conflict with data that employers need to maintain for legal compliance and/or to operate as an organization.



**The Honorable Russ Fulcher**

**At our hearing in early March, we saw how the European Union is more characterized by economies that have large businesses continuing to grow, but with fewer startups as a result of the implementation of the GDPR. In a privacy briefing for my staff, a company privacy security officer noted how GDPR is putting more emphasis on businesses to explain how they are using consumer's data and subsequently, consumers receive more pop ups as a result. Compared to ADPPA which focuses more on data minimization as its base, do sectoral laws have notice and consent fatigue as well?**

Notice and choice fatigue is real, and yes, this is an issue with the existing sectoral laws, which rely too much on opt-in or opt-out consent. Notice and choice places too much burden on the individual to protect their own privacy.

Notice, as envisioned by the GDPR's requirements around transparency, is good - it helps to set expectations and enable individuals that are so inclined to act to protect their data. Choice or consent, however, has been used in problematic ways, such as when consumers are burdened with too many choices that are too granular or layered in nature. This often leads to consumers agreeing to things without fully understanding what they are agreeing to.

The intent of GDPR was to move away from notice and choice by making consent a much more difficult standard to achieve. However, it has unintentionally resulted in the opposite effect, as more companies have sought to apply simple pop-up consent experiences to demonstrate compliance.

That is not to say that there isn't a place for notice and choice. Giving people an ability to control how their data may be used is helpful. But that should not be the end of the story.

The sorts of obligations that ADPPA would impose on organizations, including the data minimization principles and impact assessments would protect people without forcing them to make complicated decisions that they may not entirely understand or have the time to address.