RPTR KERR

EDTR ROSEN

EXAMINING LEGISLATION TO ESTABLISH A FEDERAL

COMPREHENSIVE PRIVACY AND DATA SECURITY LAW.

WEDNESDAY, JUNE 3, 2026

House of Representatives,

Subcommittee on Commerce, Manufacturing, and Trade,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:14 a.m., in Room 2123, Rayburn House Office Building, Hon. Gus Bilirakis [chairman of the subcommittee] presiding.

Present: Representatives Bilirakis, Fulcher, Dunn, Cammack, Obernolte, James, Bentz, Houchin, Fry, Lee, Kean, Evans, Goldman, Guthrie (ex officio), Schakowsky, Castor, Soto, Trahan, Mullin, Clarke, Dingell, Veasey, Kelly, Schrier, and Pallone (ex officio).

Also Present: Representatives Joyce, Balderson, Langworthy, and Fedorchak.

Staff Present: Ansley Boylan, Director of Operations; Jessica Donlon, General Counsel; Matt Furlow, Counsel; Sydney Green, Director of Finance and Logistics; Natalie Hellman, Professional Staff

Member; Calvin Huggins, Clerk; Megan Jackson, Staff Director; AT Johnson, Special Advisor; Adam Joseph, Digital Director; Daniel Kelly, Press Secretary; Brayden Lacefield, Special Assistant; Giulia Leganski, Chief Counsel; Madeline Martinez, Staff Assistant; Joel Miller, Deputy Staff Director; Lillian Noland, Clerk; Brice Ogle, Special Assistant; Evangelos Razis, Professional Staff Member; Jake Riith, Staff Assistant; Dylan Rogers, Professional Staff Member; Jackson Rudden, Clerk; Timothy Trimble, Staff Assistant; Matt VanHyfte, Communications Director; Hannah Anton Minority Policy Analyst; Jordan Antwi, Minority Intern; Keegan Cardman, Minority Staff Assistant; Kelly Fabian, Minority Chief Counsel; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; Megan Kanne, Minority Professional Staff Member; Alyssa Kimura, Minority Intern; Serena Klebba, Minority Staff Assistant; Brendan Lopez, Minority Press Assistant; Phoebe Rouge, Minority FTC Detailee; Andrew Souvall, Minority Director of Communications, Outreach and Member Services; and Hannah Treger, Minority Staff Assistant.

Mr. Bilirakis. The meeting will come to order. Good morning, everyone. The chairman recognizes himself for 5 minutes for an opening statement.

Good morning and welcome to today's legislative hearing on Federal comprehensive privacy reform. After years of debate, I am pleased to see us return to the critical issue and discuss the SECURE Data Act, legislation I believe will establish a national standard that protects American consumers and provides much needed certainty to businesses across the country.

Whether it is your favorite restaurant, your hometown newspaper, or the corner gas station, every business, no matter the size, uses digital technology these days. These innovations bring enormous benefits to everyday Americans and help ensure that our country remains dynamic and competitive in an increasingly digital world.

But today, when Americans ask if their personal data is protected, the answer depends entirely on which State they are in. Unfortunately, for the millions of Americans that live in States without a comprehensive privacy law, the answer is no. This is unacceptable as far as I am concerned, not only for consumers but for the small and mainstream businesses navigating confusing patchwork of State mandates.

The SECURE Data Act takes the best ideas of the State privacy laws and incorporates many of the ideas developed over the past several years. It seeks to establish meaningful consumer protections while creating a uniformed national standard that promotes innovation, economic growth, and regulatory certainty.

I would like to thank Dr. Joyce for leading the committee's privacy working group and all the working group members and their staff for their efforts today. I think Dr. Joyce did an outstanding job personally. This group was tasked with finding consensus on a difficult subject while balancing consumer protections with business certainty. Their work has laid an important foundation for today's discussion. I look forward to working with you, our colleagues across the aisle, and the

stakeholders, so that we work to advance the strongest bill possible.

So I want to thank everyone here on the panel, and I will yield back the balance of my time, and I will recognize the ranking member, Ms. Schakowsky, for her 5 minutes for an opening statement.

Ms. Schakowsky. Thank you.

You know, until now, Democrats and Republicans have worked together on privacy and these important issues, but right now, Democrats have really not been included, which is very distressing to me. Corporations cannot be over consumers right now.

I am going to yield right now to Rep Mullin for his comments.

Mr. Mullin. Thank you, Ranking Member Schakowsky.

Americans overwhelmingly feel powerless over how their information is collected, used, and shared, and the evidence suggests they have good reason to feel this way. Information on whether someone has been to an abortion clinic or searched for information about addiction treatment can be easily bought and sold. Cars are transmitting driver location data to insurers. Gig work platforms are using nurses' personal financial data to set individualized pay, offering lower wages to those who appear most in need of work. Foreign adversaries have legally purchased location data that can be used to track active duty U.S. servicemembers.

We know how to address these problems. My home State of California enacted the Nation's first comprehensive consumer privacy law in 2018 and has continued to strengthen those protections, giving consumers greater transparency and control over how their personal information is collected, used, and shared.

In recent Congresses, this committee has also proposed strong bipartisan privacy legislation. Unfortunately, this SECURE Data Act is not that. The legislation before us today moves in the opposite direction. It protects companies that profit from personal data, places the burden on consumers to fight for control over their own information, and undermines stronger State-level

protections already in place.

So I urge my Republican colleagues to work in a bipartisan basis on meaningful privacy protections that put consumers in control of their personal information.

And with that, I yield back to the ranking member.

Mr. Bilirakis. Does the ranking member yield back?

Ms. Schakowsky. I yield back.

Mr. Bilirakis. Okay. Thank you very much.

Now I will recognize the chairman of the full committee, Mr. Guthrie, for his 5 minutes for an opening statement.

The Chair. Thank you very much. I want to thank my good friend -- thank you, Chairman, for having us, and my good friend, Ashli Watts, CEO of the Kentucky Chamber of Commerce, for being here.

This can be a bipartisan bill. As a matter of fact, the model of this bill is what happened in our Commonwealth where we have a very prominent Democrat governor and a super majority Republican legislature that put a bill together that is very similar to what we are doing that does protect individuals, and also ensures that we can still be competitive in the world.

We are not competing with Europe to regulate. We are competing with China to innovate. We have to innovate and also protect individuals' data. So it is a crucial time, and I am glad that we are here. I believe the SECURE Data Act does protect individuals' data and allows us to flourish and to make sure we are the world leaders.

Dr. Joyce has really led this effort. Dr. Joyce, when we first started this Congress, was vice chair of the full committee and took this on. He has done a fantastic job with the staff, and I would like to yield the remainder of my time to Dr. Joyce, and thank you for the great job that you have done.

Mr. Joyce. Thank you, Chairman Guthrie, and thank you, Chairman Bilirakis. At the start of

this Congress, you gave the privacy working group a tall order. Find a path forward on Federal privacy reform that protects consumers, enables beneficial use of data, gives businesses the certainty that they need, and can earn consensus among committee Republicans.

As we saw in the 118th Congress, reaching agreement on comprehensive privacy legislation is not easy, even among Members on the same side of the aisle. We cannot and will not take that consensus for granted. The SECURE Data Act is a result of 15 months of the working group's efforts.

Reaching this consensus was only possible as strong collaboration between members of the working group who are all original cosponsors of this legislation. Thank you for your partnership, and thank you to your dedicated staff who spent countless hours on this issue. Reviewing more than 250 RFI responses, taking hundreds of meetings with stakeholders, and working through difficult policy questions to reach agreement on legislative text is no small task.

To the stakeholders who engaged with the working group, thank you for your thoughtful contributions. Many stakeholders have already expressed support of the SECURE Data Act, and I am grateful for this support as we work to move this bill through regular order to the House floor.

To my colleagues on both sides of the aisle, I look forward to engaging with you to advance the SECURE Data Act and produce the strongest bill that is possible. This legislation is built on the foundations laid by more than 20 States, red States, blue States, and purple States. The States have sketched a path forward for us that protects consumers, provides certainty for businesses, and offers a strong foundation for bipartisan Federal privacy legislation.

All of these issues are significant components of the SECURE Data Act. I look forward to today's subcommittee discussion as we work to advance this legislation. And, again, thank you, Chairman Bilirakis, and I yield back to Chairman Guthrie.

The Chair. I yield back.

Mr. Bilirakis. Thank you. Thank you, Mr. Chairman.

Give a job to Dr. Joyce, and he gets it done.

So next, I will recognize the chairman of the full committee -- actually, the ranking member of the full committee, Mr. Pallone, for 5 minutes for an opening statement.

Mr. Pallone. Thank you, Chairman Bilirakis.

When it comes to data privacy, it is clear what Americans need: They need a national privacy law that puts the focus on companies to collect and use data responsibly. They need their sensitive data used only for limited purposes that they control. They should have the ability to easily opt out across all data brokers and websites selling their data, or using it for invasive targeted ads rather than opting out one by one, and they need to know that their data will be kept safe from data breaches and misuse, and that they can pursue legal remedies if it is not. They need protections to ensure their data won't be used to discriminate against them, and our Nation's kids and teens need the strongest possible protections for their data.

Now, the Republican bill before us today does not meet that mark. The partisan SECURE Data Act is not the strong enforceable standard its sponsors describe. Instead, this bill locks in the failed notice and consent status quo, and then compounds loophole upon loophole to water down its provisions. And then, to make matters worse, it adds expansive preemptions that will leave many Americans with fewer privacy protections than they have today.

Rather than taking the strongest consumer protections from the existing State privacy laws, this bill is assembled from industry-friendly State privacy laws that have been pushed by Big Tech. It is, therefore, no surprise that this bill allows Big Tech and others to continue their ongoing privacy violations, and, unfortunately, these intrusions will only get worse as they push to insert artificial intelligence into every corner of our lives, super-charging both incentives to gather every bit of personal data and the potential harm that could result.

A future with AI Chatbox that can tailor personalized recommendations to our unconscious wants and algorithms that can set prices based on intimate details, demand strong privacy guarantees for all Americans, and, in fact, these privacy guarantees are more important than ever.

I have fought for years for data minimization standards to shift the burden of protecting Americans' privacy from consumers to the companies that profit off of their data, but the SECURE Data Act's so-called data minimization provisions, those provisions allow companies to collect and use data however they choose as long as it is disclosed in the fine print.

So this is just another notice and consent by a different name. It continues to impose unreasonable burdens on consumers. They should not be forced to become privacy policy experts every time they visit a website or download an app.

The sweeping preemptions in this bill would not only eliminate hard-won privacy protections that millions of Americans currently enjoy, but would also invalidate any State law that relates to the bill. The legislation would prevent Maryland, for example, from continuing to protect its residents by ensuring their sensitive information is not sold. It would prevent Californians from being able to delete their data from all data brokers in one step, and it would invalidate State laws on wiretapping, on robocalls, data breach notifications, civil rights, and kids' online safety.

Not only are these existing laws preempted, but States will be forever barred from addressing the future privacy harms that emerge with new technologies like AI.

So I have long supported bipartisan national comprehensive privacy legislation, but previous bipartisan compromises like the American Privacy Rights Act, the American Data Privacy and Protection Act, they recognize that a Federal privacy law must exceed the strongest protections of any State and not set a weak ceiling.

These compromises also put consumers in control of their personal information, prioritize data minimization, protecting kids and teens, and include algorithmic accountability measures. All of this was paired with strong enforcement to make these protections meaningful for consumers.

Such a compromise remains, in my opinion, the only path forward to truly protect American privacy, and I want to stress, Mr. Chairman, that, you know, though I am being very critical of this bill, I still think that we can come to a compromise similar to what we have done in the past, but this is

not it. And so I have to criticize what is here today and hope that we can work for a better bill.

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

Mr. Bilirakis. I thank the ranking member. Thank you so very much for your comments, and we will work together.

Today, our witnesses are Ms. Kate Goodloe, managing director of Business Software Alliance; Ms. Ashli Watts, president and CEO of Kentucky Chamber of Commerce; Ms. Caitriona Fitzgerald, Deputy Director of Electronic Privacy Information Center; and Mr. Tyler R. Bridegan, I hope I said that right, partner of Womble Bond Dickinson.

So let's begin with Ms. Goodloe. You are recognized for 5 minutes.

STATEMENTS OF KATE GOODLOE, MANAGING DIRECTOR, BUSINESS SOFTWARE ALLIANCE; TYLER R. BRIDEGAN, PARTNER, WOMBLE BOND DICKERSON; CAITRIONA FITZGERALD, DEPUTY DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC); AND ASHLI WATTS, PRESIDENT AND CEO, KENTUCKY CHAMBER OF COMMERCE

STATEMENT OF KATE GOODLOE

Ms. Goodloe. Good morning, Chair Bilirakis --

Mr. Bilirakis. Good morning.

Ms. Goodloe. -- Ranking Member Schakowsky, Chair Guthrie, and Ranking Member Pallone, and members of this subcommittee. My name is Kate Goodloe, and I am managing director at the Business Software Alliance, or BSA.

BSA represents the business-to-business technology providers that support companies in every sector of the economy. Privacy and security are core issues for our members, which is why we are deeply engaged on privacy legislation in the United States, including across the State capitals and worldwide.

Companies of all sizes, and in all industries, including manufacturers, automakers, hotel chains, and energy companies rely on AI-driven business-to-business tools like cloud computing, collaboration software, customer service platforms, and cybersecurity services. BSA members provide these technologies so that other companies can focus on what they do best: making products and serving customers.

The United States needs a national privacy law that is built for the modern economy, one that pairs strong consumer protections with clear rules that limit how companies can collect and use consumers' data. We welcome your focus on these issues, and I thank you for the opportunity to testify.

This committee has led Congress' work to protect consumer privacy. We urge you to continue that work and to leverage progress made by the States in recent years. In July 2022, this committee approved a comprehensive consumer privacy bill. At that time, just one State had a comprehensive consumer privacy law in force. Two years later, in April 2024, leaders of this committee released a discussion draft of an updated Federal privacy bill. At that time, five State laws had entered force. Now, two more years have passed, and 22 States have acted.

Past efforts to draft comprehensive Federal privacy legislation started from a blank slate, but the landscape of American privacy laws is no longer blank. Twenty-two States, both red and blue, have enacted comprehensive consumer privacy laws. Those laws are remarkably consistent because 21 share the same core structure with a common approach to definitions, rights, and obligations, but this core structure risks unraveling, as at least 30 different amendments have revised, expanded, and changed State laws making it hard for companies and consumers to keep up.

The SECURE Data Act adopts the right structure for protecting consumer privacy nationwide because it is grounded in the laws already passed by States. This is a key difference from prior Federal bills. The SECURE Data Act uses the same structure of privacy legislation that underpins 21 of the 22 State laws. It includes a core set of rights for consumers based on a clear consensus that consumers should have the ability to access, correct, delete, import their data, and rights to opt out of the activities like the sale of their data, targeted advertising, and certain profiling.

It also adopts the longstanding, widespread distinction between controllers and processors. This ensures its obligations fit companies across the modern supply chain in which one company relies on many others to serve customers.

I want to emphasize this last point because every company that handles consumers' personal data should be required to do so responsibly in a way that fits their goal. Grounding Federal privacy legislation in a structure already used by State laws is a critical step, and we urge you to continue this important work.

Why is it good for businesses? Well, companies should not have to track 50 moving goalposts to do business in the United States. We need a single, clear set of rules that limits how companies collect and use consumers' data so consumers trust it is used responsibly.

Why is it good for consumers? They need rights that do not depend on whether they live in one of the 22 States that is already active. Consumers' data should also be used responsibly and kept securely no matter where they live. Of course, for any Federal privacy bill to pass into law, it will need to have bipartisan support. As this bill moves through the process, we hope that the text can become a bipartisan product.

Privacy has always been a bipartisan issue. In the States, 10 Democratic governors and 11 Republican governors have signed privacy bills with this structure into law. We look forward to working with both sides of the aisle as this bill moves forward.

We appreciate the subcommittee's leadership on Federal privacy legislation, and we urge you to move the SECURE Data Act through the legislative process to promote technology adoption across the economy and protect American consumers nationwide.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Goodloe follows:]

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

Mr. Bilirakis. Thank you. Thank you for your testimony.

Now I will recognize Ms. Watts. You are recognized for 5 minutes.

STATEMENT OF ASHLI WATTS

Ms. Watts. Yes, thank you. Thank you and good morning, Chairman Guthrie --

The Chair. Good morning.

Ms. Watts. -- Chairman Bilirakis, Ranking Member Pallone, Ranking Member Schakowsky, and members of the subcommittee. Thank you for the opportunity to be here today.

I am Ashli Watts, and I am the president and CEO of the Kentucky Chamber of Commerce, which is the Commonwealth's largest business advocacy association. We represent employers of every size and every sector who collectively employ hundreds of thousands of Kentuckians.

I also serve as chair of the U.S. Chamber's Committee of 100 comprised of the chief executives of America's largest State and metropolitan chambers of commerce. Through that role, we have brought together more than 120 State and local chambers in unified support of the SECURE Data Act, including the Kentucky Chamber.

In 2024, the Kentucky Chamber played an important role as a convener throughout the State-level conversation on data privacy. We brought together stakeholders from across industry sectors, business organizations, retailers, and privacy, security, and technology experts, to negotiate a balanced workable solution. The result was House Bill 15, Kentucky's comprehensive consumer data privacy law.

Now, like Chairman Guthrie said, Kentucky is a bit of a unique State. We have a super majority Republican legislature and a Democratic governor. House Bill 15, which is very similar to the SECURE Act, passed unanimously with strong bipartisan support and was signed into law by

Governor Andy Beshear, and it is a law that the Kentucky Chamber is proud of leading the way. The goal was straightforward: Protect consumers' data and privacy while maintaining an environment where Kentucky businesses can operate and compete.

The SECURE Data Act asked Congress to extend to all Americans what Kentucky and 19 other States have already put into law. We believe that Federal action is urgent, because when every State writes its own law, even good policy creates a patchwork.

The majority of our businesses at the Kentucky Chamber are small businesses, and no business, large or small, can realistically navigate 50-State legal strategy to comply with privacy expectations. Small businesses in particular often lack in-house legal teams, chief privacy officers, or large compliance budgets.

The U.S. Chamber's empowering small business report found that nearly 2/3 of small businesses are worried that complying with different State laws will expose them to higher compliance and litigation costs, a number that jumped 14 percentage points in just a single year. A fragmented privacy landscape is estimated to cost the U.S. economy as much as $1 trillion, with $200 billion of that burden falling on small businesses.

It is important to note that strong consumer privacy protections and economic growth are not competing goals; they reinforce each other. When customers trust that their information is being handled responsibly, they are more willing to engage, to transact, and participate in the digital marketplace, and clear rules help build that trust.

The SECURE Data Act is built on bipartisan State laws just like the one we passed in Kentucky. It provides consumers with strong privacy protections, the right to access, correct, delete, import their data, opt out rights, and opt in requirements for sensitive information. It has a reasonable data minimization standard, and it establishes a national standard without a private right of action.

Every State that has passed this type of legislation has made that same choice, because it produces consistent, meaningful outcome for consumers. This framework has been signed by 9

Democratic governors and 11 Republican governors. More than 2,500 State lawmakers, both Democrats and Republicans, have voted for it. More than 135 million Americans are already protected by it.

This is not just a technology policy issue. It is a competitiveness issue. Kentucky's businesses and all American businesses, especially small businesses, need one clear set of rules of which they can build around. The SECURE Data Act provides just that. The model is proven, and the consensus exists across party lines. What remains is for Congress to act.

On behalf of the business community, I urge this subcommittee and the full Congress to pass the SECURE Data Act. The Kentucky Chamber of Commerce, the U.S. Chamber of Commerce, and our more than 120 State and local chamber partners stand ready to support you in this effort.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Watts follows:]

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

Mr. Bilirakis. I tell you what, that was excellent testimony. I appreciate it.

Ms. Fitzgerald, you are recognized for 5 minutes.

STATEMENT OF CATRIONA FITZGERALD

Ms. Fitzgerald. Chairs Guthrie and Bilirakis, Ranking Members Pallone and Schakowsky, members of the subcommittee, thank you for the opportunity to testify today. My name is Caitriona Fitzgerald, and I am deputy director of the Electronic Privacy Information Center, or EPIC.

EPIC is an independent nonprofit established in 1994 to secure the fundamental right to privacy in the digital age for all people, and we have been deeply involved in the debate in the States over privacy legislation. We believe privacy is a fundamental human right.

There is broad bipartisan agreement that Americans need stronger privacy protections. Poll after poll shows that consumers are fed up with the status quo. They don't want surveillance pricing at the grocery store. They don't want their cars broadcasting their driving habits to their insurance companies, and they certainly don't want U.S. troops put at risk in war zones because online advertising is a privacy nightmare.

America needs a strong data privacy law, but the SECURE Data Act is not the right approach. This committee previously approved bipartisan bills that meaningfully protected privacy. In those negotiations, both sides worked to craft a Federal bill that was stronger than the strongest State law. Those bills included meaningful data minimization, heightened protection for sensitive data, limits on data discrimination, and robust enforcement.

The SECURE Data Act does the opposite. It sets a national standard that is weaker than the weakest State law. We shouldn't be making the floor the ceiling. You have heard today that this framework has been sufficiently in the States, but it hasn't been sufficiently for the people in those

States.

What makes it so weak? A core weakness of the SECURE Data Act is its lack of a real data minimization rule. The SECURE Data Act allows businesses to continue collecting and using data however they please as long as they disclose it in a privacy policy that we know few consumers read, and no consumer has the power to change. Data minimization only works if it actually limits how much data companies can collect and how they can use it.

Now, my 8-year-old is a huge soccer fan, but every team he joins requires me to download a new app to get the schedule and talk to the coach. If I don't like the app's terms, there is no "disagree but download the app anyway" button. There is I have to accept it or not download the app. Am I supposed to tell my son he can't play soccer because his mom doesn't want her data used to train AI systems? Congress shouldn't be passing a privacy law that bakes this unfair system where companies get to dictate the terms into law.

The SECURE Data Act also fails to adequately protect our most sensitive data, like our location data. Sensitive data should have stronger protection than beyond simply consent because, in practice, that just leads to endless pop-ups that consumers grow numb to.

Another significant weakness of the SECURE Data Act is that despite its focus on individual consumer rights, it lacks a private right of action. If a company ignores my request to delete my data or opt out, there is no recourse. It is essentially unenforceable. The FTC and State AGs don't take on individual cases.

This bill has many more weaknesses than I have time to detail in my testimony today, but the fatal flaw is the combination of these weak rules with the most expansive preemption option available to the Federal Government. This bill would wipe out decades of State laws causing chaos in our legal system.

My testimony includes a list of the hundreds of laws EPIC believes could be preempted, including those on robocalls, civil rights, kids' online safety, and even longstanding privacy torts.

This bill would also make it harder to hold Big Tech accountable in court. Just last week, Meta, Snap, YouTube, and TikTok, agreed to a $27 million settlement with a Kentucky school district where platforms' addictive designs harm students' mental health. Many of the claims in that case relate to rules in this bill. So there is no way of knowing whether similar cases could move forward.

The weak rules in this bill paired with its extreme preemption provision would be a disaster for Americans. I want to emphasize that. The passage of this bill would be a worse outcome for Americans than no Federal data privacy law at all.

The trends in the U.S. are clear. Companies are abusing increasing amounts of our personal data. AI is turbocharging that abuse, and Americans want more protections from Big Tech. Yet, this committee is proposing weaker legislation than it overwhelmingly approved in previous sessions.

Congress should not pass a privacy law that fails to address the very real data abuses and privacy harms that Americans are asking them to fix, and it certainly should not strip Americans of privacy rights they already have. We know what is needed: Strong data minimization, heightened protections for sensitive data, limits on data discrimination, and robust enforcement.

The SECURE Data Act, unfortunately, doesn't meet the moment, but the solutions do exist, and I urge this subcommittee to consider other approaches that give Americans a privacy they want and deserve.

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

[The prepared statement of Ms. Fitzgerald follows:]

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

Mr. Bilirakis. Thank you.

Now, I will recognize Mr. Bridegan for your 5 minutes. I appreciate it.

STATEMENT OF TYLER BRIDEGAN

Mr. Bridegan. Chair Guthrie and Bilirakis, Ranking Member Pallone and Schakowsky, and members of the subcommittee, my name is Tyler Bridegan. As a brief housekeeping matter, I am here in my personal capacity today, not on behalf of any company, organization, or client.

One, I want to say thank you, members, for picking up this effort again. I think we all are in agreement that it is an essential priority to get a Federal privacy law passed in the United States.

I want to start with a bit of my background so you can understand the sort of lens that I am viewing, the SECURE Data Act. Up until the end of last year, I was serving as the director of privacy and tech enforcement for the Texas attorney general's office. There I headed up our efforts to implement and enforce all of the recently passed Texas privacy laws. That included comprehensive privacy, data broker laws, children's privacy, and online safety laws.

As part of that, we took a very intentional approach to looking at sort of what harms exist in the United States. Many of our cases were very high profile. They involved looking into the entire auto manufacture industry and several social media companies, and several of our investigations ultimately led to litigation.

Also as part of my role, I have the opportunity to get to know my counterparts in other States. It was an incredible experience getting to hear what so many States are doing on the privacy front, both advising their legislatures on what is working and what isn't in their privacy laws, as well as figuring out ways to appropriately enforce their law and dedicate resources.

At the end of last year, I returned back to private practice at the law firm Womble Bond

Dickinson. Our firm has a very broad client base. We have our origins in the southeast, and then we have since expanded across the United States. As part of that, we have clients of all sizes that are in every industry from your brick and mortar to defense, you know, to giant online retailers.

It has been extremely educational for myself to see what all of these different companies and different sectors care about with respect to privacy. But enough about my background.

On the SECURE Data Act front, I want to cover four key points with you guys today. First, there is widespread support, and I think that has been echoed by all the other witnesses that Americans want a privacy law passed. Companies' practices are unclear to consumers. They are learning of new ways their data is being used. It is time to protect those consumers.

In Texas, as part of our privacy law, we had to create a consumer privacy complaint database. It went online July 1. By July 2, we had our first 10 consumer complaints coming from corners of Texas you would not expect. Someone from Laredo filed a complaint asking for a fast food chain to update their privacy policy because it didn't have an option for them to delete. Not the first company I probably would have looked into. All to say, there is widespread support on that front.

The second point, we now know much more tangible harms. Several of our cases focus on how data, particularly sensitive data types, were ultimately being used to monetize or affect consumers.

Third, we now know more. The last time Congress pushed forward with this effort, most of the State laws were not in effect, and there has definitely not been enforcement that it occurred yet. We now have had the opportunity to see which provisions in the laws sort of protect from those key consumer harms, particularly the tangible harms that we are seeing emerge.

And then fourth, I think passing a Federal privacy law is crucial. Right now, over half the States don't have sensitive data protections meaning, by default, companies can collect and use that data however they please. Trillions of data points are being generated about Americans every single day that still go unregulated.

All that to say, I am extremely excited for this effort to be moving forward. I think we are actually pretty close on a lot of provisions, which is exciting when I was reviewing this law.

That is it for me, and I am happy to answer any questions.

[The prepared statement of Mr. Bridegan follows:]

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

Mr. Bilirakis. I thank the gentleman.

And now I will begin questioning and recognize myself for 5 minutes.

I share the concerns of many Americans that companies are collecting more personal data than is really needed. At the same time, we have seen how overly restrictive privacy laws, like Europe's general data protection regulation, throttle privacy, again, private industry and innovation.

So Ms. Goodloe, how do the SECURE Data Act's restrictions on data collection work? And how do they differ from Europe's law and past proposals before the committee?

Mr. Bridegan, if you want to add something after Mr. Goodloe, we would appreciate that as well.

It is actually Ms. Goodloe. I apologize.

Ms. Goodloe. That is all right. Thank you for the question.

The SECURE Data Act builds on the experience of State laws to create a core set of rights for consumers and a core set of obligations on companies. Importantly, those obligations extend across the modern supply chain, and they create rules for both controllers, which are the companies that decide how and why to collect consumers' data, and for processors, which are the companies that handle data on behalf of other companies pursuant to their instructions.

That is a critical difference from prior Federal laws, and it ensures that the obligations created by this act carry across the modern economy. I think it is important that Congress pass a law that creates one set of rules for companies to collect and use data so that consumers know it is used responsibly.

Mr. Bilirakis. Thank you.

Mr. Bridegan, would you like to add to that?

Mr. Bridegan. Yes. Compared to the GDPR, it is actually conceptually similar. There are similar restrictions in the GDPR about sensitive data and using consent in order to collect and use

that data. That is present in the SECURE Data Act. There is a long history: Illinois' Biometric Information Privacy Act, Washington State's most recent My Health My Data Act, Texas' similar Biometric and Genetic Privacy Act. That principle is strong. It has led to several of the largest settlements in history in the United States.

I would also say GDPR takes a more high-level approach without being too prescriptive, and that is similar to things we have seen in other context in the United States, like the NIST cyber controls. It is explaining what types of controls you need and what sort of practices ultimately lead to stronger protections without being so prescriptive as to require companies to implement or include many specific requirements in the privacy policy, for example.

Mr. Bilirakis. Thank you.

Next question: There is a view in Washington, as well as some States, that more mandates on business means more protections for Americans. Right now we have 22 comprehensive consumer privacy laws in this country, which may become 24 in short order as governors of Louisiana and Vermont sign the bills on their desks, and I know you alluded to this earlier.

But these are laws that sit alongside existing Federal requirements for different sectors, such as healthcare and finance and FTC, the FTC Act. So, Mr. Bridegan, is the status quo effectively protecting consumers? Are more State-by-State laws better than a uniformed Federal framework?

Mr. Bridegan. I think there has been a good movement at the State level to increase enforcement. That said, at the end of the day, 50 States having a uniformed law to enforce and create precedent around, plus being able to team up with the Federal Trade Commission will create very clear market shifts in privacy practices around the country.

Most companies want to in good faith comply with the law, but at the end of the day, there is a real effect when there is a heightened risk of enforcement from several entities. I think a Federal law would create that heightened risk for enforcement and ultimately encourage companies to prioritize complying with the letter of the law.

Mr. Bilirakis. I have a little more time. Ms. Goodloe and Ms. Watts, would you like to add anything?

Ms. Goodloe. I will add that the important piece of a national law is it will protect consumers nationwide. Right now consumers are protected in 22 States with different State laws, and we need a clear set of national rules that companies can build strong compliance programs toward. I think that will make sure that consumer protections are extended nationwide and that companies know what to do and what to focus on to better protect consumers.

Mr. Bilirakis. Ms. Watts?

Ms. Watts. Yes. Thank you, Chairman. I would echo my colleagues' answers on that. We, in Kentucky, really did kind of question whether we should continue to advocate for a Federal law or work on a State law. After several years of no action by Congress, we decided that we needed to take matters a little bit into our own hands and pass a law in Kentucky, but we absolutely believe that a Federal law is the way to go.

I am proud to speak on the majority of my members of the Chamber of Commerce for Small Businesses. They want one clear set of standards to be able to comply with, and this is what this bill would do instead of the patchwork of all the various States.

Mr. Bilirakis. Very good. Thank you.

I yield back the balance of my time, and I will recognize the ranking member of the subcommittee, Ms. Schakowsky, for 5 minutes of questioning.

Ms. Schakowsky. Ms. Fitzgerald, I wanted to ask you -- where are you? There you are. How does this bill benefit corporations rather than the American people?

Ms. Fitzgerald. Thank you so much for that question, Ranking Member Schakowsky, because I think it is really important for members to understand a bit of the history of where these 22 State laws came from.

Privacy and consumer rights and civil rights groups have opposed those laws in the States.

Those bills originated from a draft that was written by tech giants in Washington State. It ultimately did not pass in Washington State, but they took it to Virginia first. It passed in 2021, and then they brought it to, you know, these now 22 States or 21, I guess, because California followed a different path, and pushed their weak model with the hopes of getting exactly to this moment, coming to Congress and saying, This is the consensus in the States. Please pass this at the Federal level, and preempt States from doing anything for all of the time on privacy.

Those State laws are far too weak to adequately protect privacy, and Congress should not be emulating that model, right. Privacy laws should not be written by the very entities they seek to regulate.

This bill also contains about five pages of exemptions and loopholes, corporate carveouts. It makes you wonder who the weak rules in the bill will even apply to in the end. So that is something we really want to be careful of when we are looking at bills as well and who they are protecting.

I will say, as a private entity advocate in the States, it is disappointing to see how quickly the conversation turns to a focus entirely on business compliance, and consumers are -- you know, they are hardly mentioned in the end. You almost would forget that you are working on a consumer protection bill in the end, as opposed to a business compliance bill.

So I will say so much work was done on previous bipartisan proposals to come up with a framework that protected Americans and allowed businesses to thrive and innovate, and it is disappointing that the SECURE Data Act throws all of that out and starts over. And I hope that we can come back to the table and come to a bipartisan agreement on a bill that works for both the American people and our businesses.

Ms. Schakowsky. Are there other things we should be doing to make sure the consumers are benefited?

Ms. Fitzgerald. I think the key with the privacy law is to make sure that the onus of protecting privacy is not entirely on the consumer, and rather, the businesses that are collecting,

using, profiting off of our data have obligations on the forefront to limit the amount of data they are collecting and using. There is just such a power imbalance that if companies could just write these policies and say take it or leave it, that just doesn't protect privacy.

You know, I realize that we are trying to put things back in the box because we didn't act on privacy early on. We have been asking Congress to pass a privacy law for 30 years, but that doesn't mean that we should just allow the status quo to continue. We need, consumers need adequate protections online, and I really do think that the solutions exist to do that in a way that would allow our businesses to thrive but adequately protect consumers.

Ms. Schakowsky. What are the things that we need to do to make sure the consumers are empowered?

Ms. Fitzgerald. We need a strong data minimization rule that limits data collection and use. It says to company, you know, the ADPPA and APRA, limit data collection use to what was necessary for the product or service the consumer is asking for.

So that means that companies have to better align their data practices with what consumers expect.

I don't expect my flashlight app to collect my location data. I expect my weather app to collect my location data, but I don't expect them to sell it to a dozen data brokers. So we want to better encourage companies to have this culture of privacy where they are only collecting what they need to provide the service the consumer is asking for.

Ms. Schakowsky. Thank you. I appreciate that very much.

Mr. Bilirakis. The gentlelady yields back.

I now recognize the chairman of the full committee, Mr. Guthrie, for his 5 minutes of questioning.

The Chair. Thank you very much.

And the process by writing this bill that Ms. Fitzgerald described absolutely was not the

process in writing this bill. Dr. Joyce will speak for himself, but we met with hundreds of different people, different groups, and everybody on here wants people's data to be secure and to have their privacy and have that security.

As I said, we are not looking to compete with Europe to regulate. We are looking to compete against China to innovate. And we don't want to be China either. We certainly don't want to be Europe, and so the question is, can you find a balance? And that is what we have worked hard to find a balance, and we strongly believe that we have.

Europe and the United States had the same economy 20 years ago. The same economy 20 years ago, the European economy. And there are a lot of reasons. Our energy policy can't dismiss that Britain has pulled out, but our economy is twice the size of Europe today in 15 years, twice the size.

So now you have to look at the reverse. What if our economy today was half the size that it is today? You talk about unemployment. You talk about affordability. You talk about all of these. So these things matter. And things just don't happen in a think tank. Things just don't happen in academia. Things happen in the real world.

So people's data is being collected in the real world, and people are trying to innovate and grow their companies in the real world. So how do we strike that balance? That is what we are looking at.

So Ms. Watts, we heard a lot about Big Tech. I know in Kentucky we have a lot of small businesses, and you mentioned it in your remarks. Could you go a little further on how typical Kentucky small businesses are affected by this and why they -- and I don't believe Governor Beshear was out looking for Big Tech and for businesses. I think he is trying to make Kentucky a business State. I am not saying he was anti, but I don't think he was saying how can we give everything to Big Tech. I don't think he had that at all.

And it didn't just come from the general assembly because he has been known to veto a lot of

bills. They get overwritten, but he vetoes a lot of them. So I would have to think that he had a hand in doing this, too. So I don't think he is out there trying to protect Big Tech at the expense of the consumer, as has been insinuated.

Ms. Watts. Absolutely. Thank you, Chairman Guthrie, for that question.

You know, we are really proud of our small businesses in Kentucky. They are the backbone of our economy, as you know in your district. And I always say I have been at the Kentucky Chamber now for 14 years leading their advocacy. I feel like I am pretty good at my job, but it is still really hard to pass a bill unanimously through the Kentucky general assembly and have it signed into law by a Democratic governor. I think that shows the power of our convening and the power of the consensus that we built around this.

It was not just Big Tech. Of course, we had tech at the table. We needed to have their voice be heard, but we also had small businesses. We had retail. We had restaurants. We had consumers. We had everyone at this table really working together for a consensus-based solution, and that is exactly what we did in Kentucky that is really mirrored here with the SECURE Act.

So I think just speaking for -- it wasn't only bipartisan. It was unanimous in Kentucky general assembly and then signed into law by Governor Andy Beshear.

The Chair. Because every business, no matter what size, if they have a credit card portal, is affected by this.

Ms. Watts. Exactly.

The Chair. If you have a loan, a person with a store, and your family runs your store, and you have a credit card portal, which everybody has to have now, then you are affected by this bill.

Ms. Watts. Absolutely, and I think small businesses --

The Chair. Or any proposal that we do.

Ms. Watts. Exactly.

Small businesses in your district and throughout the Commonwealth want to be a nationwide

marketplace. We do a lot of our shopping online. You want that ease, and you want your small businesses in the Commonwealth to grow.

The Chair. And I was in the general assembly. So being a product of the general assembly, you do get a lot more grassroots input. So my guess is you had a lot of consumers, and you had a lot of businesses around the table, as opposed to consumer groups that represent the interest of consumers, not out there as think tanks. You always have to wonder who hired the think tank.

And the second thing is Big Tech. Not in Kentucky. You didn't have probably the four or five big titans or Big Techs sitting at the table with a bunch of consumer groups; it was consumers and small businesses.

So if you see one of these State laws have developed the way that they have, my guess is because they are listening to the people in their State, not because they are just trying to cover up for some other Big Tech, as has been insinuated here today.

Ms. Watts. I would absolutely agree, and I would say if small businesses were upset with a law that was passed in Kentucky 2 years ago, I absolutely guarantee you that law would not have been passed unanimously by the Kentucky general assembly and signed into law by Governor Andy Beshear. Small businesses in Kentucky supported this bill. Local Chambers of Commerce all across the Commonwealth supported this bill, and that bill has now been mirrored a lot in the SECURE Act.

I think we are a great example to show the convening power and the consensus bill that we built around data privacy in the Commonwealth.

The Chair. And it is typical of State governments to have those kind of grassroots in play.

Thank you. I don't have time to ask another question. I yield back.

Mr. Bilirakis. You are welcome to ask another question, Mr. Chairman. All right. The gentleman yields back.

Now I will recognize the ranking member of the full committee, Mr. Pallone, please.

Mr. Pallone. Thank you, Chairman Bilirakis.

I have long said that the core of any comprehensive privacy standard has to be with a strong data minimization, but if the SECURE Data Act contains a provision that claims to offer data minimization, that actually allows companies to do anything they want with consumer data with notice and consent.

So my question, Ms. Fitzgerald -- I actually have four. So I am going to ask you to answer them in a minute or so if you could. So the first one is: How does the standard for data minimization in the SECURE Data Act compare to the data minimization offered by prior bipartisan Federal privacy proposals, like the American Data Privacy Act and the American -- well, the two bills, the American Data Privacy and Protection Act and the American Privacy Rights Act? And does it provide, the SECURE Act, any meaningful difference for consumer privacy compared to the status quo? In a minute.

Ms. Fitzgerald. Thank you, Ranking Member Pallone.

I think we use data minimization as the most important substantive rule in any privacy bill, and I would hesitate to call what is in the SECURE Data Act data minimization. I know that section is titled that way, but it is really data maximization. Companies are incentivized to write their privacy policy as broadly as possible, list as many perks as is possible because the only thing that counts as a violation is not disclosing.

So they will just say we collect your data for marketing purposes. That allows them to do anything and doesn't tell anything to consumers. In fact, it is basically restating current consumer protection law. So it is not giving them any additional protections because unfair and deceptive trade practices laws already require companies to be truthful in their privacy policies.

Whereas, previous bipartisan proposals, like you said, limited -- required companies to limit their data collection and use to purposes that the consumer expected, that were reasonably necessary for the product or service they asked for.

Mr. Pallone. All right. Thanks.

So the second thing is about enforcement, because meaningful consumer protection is only as effective as its enforcement, and that includes cases involving individual consumers who have been uniquely harmed. So the question is how would the lack of a private right of action in the SECURE Data Act impact the laws affecting us? Will the right to cure further impact the law's effectiveness, and in what way?

Ms. Fitzgerald. Yes, thank you.

We have seen in the States that the lack of a private right of action, without it there is really little incentive for companies to comply with the law because they know the risk of government enforcement is so low, and that is only made worse by the inclusion of a right to cure in the SECURE Data Act because companies know they will get a get-out-of-jail-free card. If government enforcers do come knocking at their door, they can just fix the problem, and there can't be any enforcement.

Consumers lose in all these situations, because they can't enforce their own rights, and then if the government agency, a State AG or the FTC does try to enforce, companies can just fix the problem after the fact even though the harm is already done. Your data is already out there. Your privacy rights have already been violated, and there is no getting that back.

Mr. Pallone. All right.

And then the third thing, I recently began an inquiry into surveillance pricing to find just how widespread these practices are, and this includes pricing that can use consumers' intimate details to predict when they are most vulnerable and most likely to pay for the product.

So the question is, would the SECURE Data Act address the problems presented by surveillance pricing algorithms and practices?

Ms. Fitzgerald. No. The SECURE Data Act does nothing to address surveillance pricing. Companies could just say in their privacy policy that they were using your personal data to offer personalized pricing. And what that would look like for the consumer is, they sign up for a loyalty program in the hopes of saving money, and then their personal data is used to determine just how

much they will tolerate paying for eggs, which could be a different price than their neighbor. And the SECURE Data Act would do nothing to stop that harmful practice.

Mr. Pallone. All right.

And then the last thing is about preemption. The SECURE Data Act contains very broad preemption language that goes beyond what we saw in APRA and the ADPPA, and clearly preempts more than State comprehensive data privacy laws. So the question is under the SECURE Data Act, what is the potential scope of State preemption, and how might this affect consumers in States that already have strong protections in the law?

Ms. Fitzgerald. Yes, the SECURE Data Act includes the broadest preemption option available to the Federal Government, preempting anything that relates to the provisions in the bill, and the Supreme Court has described this form of preemption as deliberately expansive.

I attached a list of the hundreds of laws that EPIC believes to be preempted to my testimony. That is even a representative list. There could be many more. It is hard to overstate the chaos this will cause in our legal system. You know, it goes so far beyond just preempting the comprehensive privacy laws that it attempts to mirror. It would preempt longstanding privacy torts. It would preempt a lot of kids' online safety laws, like age appropriate design code, laws about robocalls that we all -- no one wants robocalls back, and data breach notification laws.

So the preemption provision was just written so expansively that everything from, you know, kids' online safety to robocalls is at risk.

Mr. Pallone. All right. Thank you so much. Thank you, Mr. Chairman.

Mr. Bilirakis. The gentleman yields back.

I now recognize the gentleman from the great State of California, Mr. Obernolte, for his 5 minutes of questioning.

Mr. Obernolte. Thank you, Mr. Chairman. Let me begin by saying how delighted I am that we are finally having this hearing. This has been a long road. It has been an honor for me to serve

on the data privacy working group under the leadership of Congressman Joyce.

Let me emphasize some of the points that have already been made here. This legislation has been over a year in drafting, and we tried to correct some of the mistakes that had been made in previous efforts by broadly engaging all corners of the stakeholder community. We sat down with hundreds of different groups representing different points of view. And I want to give a shout out to all of our individual staff and the committee staff, because this has been a Herculean effort to get to this point.

One of the things that I think we need to spend more time talking about is how burdensome it is on small businesses to have this complex regulatory landscape of potentially 50 different State laws, currently 22, but potentially 50 different State laws. As a technology entrepreneur myself, I can tell you that a landscape like that is a barrier to entry to people trying to start new businesses and technology because what it does is it advantages Big Tech because those are the companies -- not to pick on them, but those are the companies that have buildings full of lawyers and the sophistication to deal with a regulatory landscape like that.

So if you are Google, if you are Microsoft, you can do it. If you are two people in a garage somewhere trying to start the next Google or the next Microsoft, you can't. And this is the big challenge that we are trying to solve with one unified Federal standard.

So Ms. Goodloe, you have many small businesses as part of your organization. Can you talk about just how challenging it is to navigate this landscape of currently 22 different State regulations?

Ms. Goodloe. Thank you for the question.

BSA represents the business-to-business technology providers that power companies across every sector of the economy, and those are companies of all sizes. When you have to comply with laws on a State-by-State approach, companies are forced to track 50 moving goalposts. We have 22 State laws already enacted, several more awaiting action by governors, and amendments that continue to go through the legislative process every day. It is a complicated landscape no matter

what size your company is.

I can only speak for the business-to-business part of the technology industry, but we think one standard is needed, so that companies of all sizes know the rules and know how to comply with the goal of protecting consumer privacy so that consumers trust that their data is used responsibly.

RPTR SCHWALM

EDTR CRYSTAL

[10:14 am].

Mr. Obernolte. All right. Well, obviously, I would very much agree with you.

Ms. Fitzgerald, we could agree to disagree on some of these issues. You said a couple of things that I found to be kind of inflammatory. I wanted to talk about them and give you the opportunity to respond.

One of the things you said is that the goal of this process of creating one Federal standard should be to create a standard that is stronger than any of the individual State standards. I very much disagree with that because we tried very hard to take a consensus approach where we took the best of what every State had to offer, and that would mean being somewhere in the middle, not the strongest, not the weakest, but looking at what worked.

The other thing that you said that I take issue with a little bit is you said that this bill is weaker than the weakest State standard and that we would be better off to have no Federal standard at all than to pass this bill.

I do take exception to that because, first of all, the weakest State standard right now is no State standard. We have 22 different State standards. That means the majority of States have zero protections for consumers when it comes to digital data privacy.

How can you say that having no bill is better than the protections in this bill even if we agree to disagree on how strong those protections should be?

Ms. Fitzgerald. Thank you, Representative. Thank you for the opportunity to elaborate on this.

We believe at EPIC, especially where there is a broad preemption provision in this bill, that if Federal law does not exceed the protections in the strongest State law then Congress is taking away privacy rights from Americans that they already depend on.

Mr. Obernolte. Yeah, but half the States only have -- they have no privacy rights in half those States. So even if that is true, you are giving privacy rights to consumers that right now have none.

Ms. Fitzgerald. But privacy rights that are not necessarily meaningful. In practice, most businesses are now offering these consumer rights of access, correction, and deletion to residents of 50 States because so many States have the State privacy laws that include these consumer rights. So in practice the enactment of this bill is going to give Americans, even in States without privacy laws, very few rights that they don't already have today.

Mr. Obernolte. Well, I mean, the whole goal here is to create one Federal standard that gives everyone the same rights that we all believe that we should have.

And I am hopeful, Mr. Chairman -- I see my time is expired -- I am hopeful that we can get to a place of bipartisan agreement on this. Obviously, for this to be a lawmaking exercise, we have to get there eventually. So I hope that we can still continue having this discussion as the bill moves forward.

I yield back.

Mr. Bilirakis. Good enough.

I now recognize Ms. Castor for her 5 minutes of questioning.

Ms. Castor. Well, Mr. Chairman, I am not going to mince words. I think this is bill is an appalling betrayal of hardworking Americans and their ability to safeguard their personal information. It is a violation that would just allow violation of their privacy to continue.

It wipes away laws across the country that protect privacy. It will lead to higher costs for consumers. It will further unleash insidious AI surveillance pricing. It will end State laws relating to unwanted robocalls and spam text messages. And it will gut online privacy protections for kids.

Ms. Fitzgerald, you have an entire section in your testimony about how the GOP anti-privacy bill will make minors less safe online. We have debated this a lot in this committee. Will you

expand and elaborate on that?

Ms. Fitzgerald. Yeah. Sure. Thank you for the question.

States have passed dozens of laws giving kids and teens stronger privacy protections online, both as part of comprehensive privacy laws and in age-appropriate design codes and other kids online safety rules, and this bill will take those protections away without really meaningfully replacing them.

So it is an example of why I did say that I do think that passage of this bill would be a worse outcome for Americans because we know how this works. If this privacy bill passes, Congress will have checked the box on dealing with privacy for decades to come and these rules will be cemented into law.

Technology is changing. We are already seeing the harms that kids are suffering, especially kids are suffering online due to the harmful business practices of big tech. And I just don't think that Congress should be passing a Federal privacy law that fails to address those harms.

Ms. Castor. And it would weaken enforcement of those laws, kind of gut those enforcement mechanisms. In fact, there are many lawsuits right now that parents and families have brought against the tech companies. What would the impact be legally?

Ms. Fitzgerald. Yeah, the broad preemption provision in this bill would really cause chaos for those lawsuits because you are talking about school districts and parents and others going against the most powerful companies in the world.

And so if those companies have an out to argue in court that their claims are preempted by this bill and that they disclosed in their privacy policy what they were doing, there is a question about whether --

Ms. Castor. I think that is so wrong, that is so wrong, to rip the rug out from under the families and kids. I mean, the evidence of harm to children online is very apparent after many years.

And I know they want to -- I hear the argument. They want to hang their hat on, okay, we want one set of rules nationwide, but if you have a very weak Federal standard, that is no protection at all for people's privacy. Is it?

Ms. Fitzgerald. No, it is not. I agree that we need a Federal data privacy law and I have been asking that for 30 years. But we need that rule to be strong.

Ms. Castor. In fact, we had a good bipartisan compromise that we had hammered out here.

I think that Americans deserve better. They really do deserve to be able to safeguard their personal, private data. Some of it is very sensitive. Their personal health data as well. And this would just, I think, unleash the big tech companies' ability to mine that data, make us the product, with no recourse.

It is kind of on theme for what this committee has done. If folks don't know what this committee has done this session, they passed out of this committee a complete ban on any AI regulation at all -- at all -- federally or for the States -- at all.

They have also gutted our Kids Online Safety Act that is very bipartisan in the Senate. Also, the kids online privacy protection act passed by unanimous consent in the Senate. And here, I don't know why, the tech companies have greater influence. They have gutted that, weakened that.

It just seems like it is another gift to the big tech companies. It is unfortunate that that is the tack of this committee, but I want folks to know what is going on here.

I just think people deserve better. They deserve to have their privacy protected and not constantly mined and surveilled and then sold.

And I will end it there. Thank you very much.

Mr. Bilirakis. The gentlelady yields back.

We will recognize Mr. Bentz for 5 minutes of questioning.

Mr. Bentz. Thank you, Mr. Chair.

Mr. Bridegan, just to start with you. This is just a question I have had for years.

You say on page 4 of your testimony, "Consent is generally defined as a 'clear affirmative act that signifies the customer's freely given, specific, informed, and unambiguous agreement to process their personal data.'"

I don't know how many times I have quickly gone through the 26 pages -- 56 pages of the consent in other situations and gone to the bottom box and checked "yes."

I am just curious how you or anybody would ever suggest that we are going to get this kind of understood consent from anybody in these kind of situations.

Mr. Bridegan. Yeah. Thank you for the question.

I would like to clarify a couple -- respectfully -- a couple misunderstandings on how consent works in these privacy laws.

So Texas has a very similar comprehensive privacy law as the SECURE Data Act, particularly around consent and sensitive data.

Texas is also the only State in the United States that has recovered over a billion dollars multiple times using laws that are based on consent. There is no other State that has ever recovered more than a billion dollars from a company.

So consent in these scenarios is not something as simple as a click-through when you see a banner at the bottom of the screen and say "accept all" to privacy policies. It needs to be specific and informed.

Texas courts have done a great job on explaining that each one of these adjectives has a meaning and a company needs to satisfy those specific meanings. So at a minimum you are going to need to be able to demonstrate that the company disclosed what they were collecting the data for and how they were using that data.

Mr. Bentz. If I may, I understand the desire to achieve that type of understanding, but what are the odds of that actually happening?

Mr. Bridegan. Well, part of that relates to the enforcement mechanisms, right? So if there

is actually the risk of enforcement, companies are going to take a close look at what they are disclosing and telling consumers and how they are obtaining consent.

Mr. Bentz. Well, if I may, the way this works, you harvest this data from millions of people. And so to suggest that these companies are going to go to millions of people and ascertain that each one has reached that level of consent seems highly unlikely. So I am just trying to say, can you explain to me how we are going to reach that level of consent in any meaningful form?

Mr. Bridegan. It would be on a going-forward basis, obviously. But a company would need to -- say if it was just a website that wanted to collect sensitive data, that is when you need -- our position was always that it needed to be a separate disclosure. In a short disclosure, not something that is mixed into a giant privacy policy that nobody reads, it needs to be something that is very clearly informing the consumer. And so that is like you could condense that down to two sentences, but it does need to specifically state, like, we are collecting your geolocation data.

Mr. Bentz. If I may, I don't want to be too mean to my State of Oregon, but our reading comprehensive test scores are abysmal. So I wonder how anybody is going to read these kinds of things in my State of Oregon and actually understand them.

But I want to set that aside, but it is a terrifically important question, because the whole system now seems to be run on LLMs, and that means all kinds of data. And what you are basically saying is, there is going to have to be an opt-in from an educated person who actually gets it, and I don't see that happening.

Mr. Bridegan. I mean, under the law, the burden is on the company to demonstrate that they actually attained specific informed consent. So they are going to have to be adversely arguing that with the regulator. So that is a burden shifting. It is not as simple as a notice provision. But that ultimately will fall on -- that burden to demonstrate that will be on the company.

Mr. Bentz. Ms. Watts, a State-by-State regime rewards whoever has the biggest legal and compliance budget, and that is rarely a new entrant. This goes back to comments already made by

previous folks.

So my question is, does a privacy patchwork entrench the largest incumbents at the expense of smaller competitors? It seems to be the answer is obviously yes, but go ahead and tell me.

Ms. Watts. Yeah. We absolutely agree that a Federal framework is really the way to go for small businesses. As we have discussed several times throughout this committee testimony, the compliance set for small businesses, the navigation, is really cumbersome and burdensome. So we do believe that a national framework will help small businesses.

Mr. Bentz. Thank you.

And I just want to thank the panel. Extraordinarily interesting conversation. I appreciate it very much.

Yield back.

Mr. Bilirakis. Thank you. Appreciate it.

I now will recognize Mr. Mullin for 5 minutes of questioning.

Mr. Mullin. Thank you, Mr. Chair.

And thank you all for your testimony today.

As I mentioned earlier, I am concerned that the legislation before us today moves us in the wrong direction on data privacy. Not only does it set a remarkably low ceiling for privacy protections, it also overrides the good work that those States have been doing in this arena.

As I noted, California has enacted some of the strongest privacy protections in the country, giving consumers rights over how their personal data is collected, used, and shared. These laws are now actively being used by Californians to exercise control over their data.

For example, California also recently enacted the Delete Act, which allows consumers to submit a single request directing registered data brokers to delete their personal information. Hundreds of thousands of Californians have already used this service, and Connecticut adopted similar legislation just last week, as I understand it.

Ms. Fitzgerald, can you discuss how the legislation before us today would affect existing privacy protections for Californians?

Ms. Fitzgerald. Yes, it would completely wipe out the protections in the California Consumer Protection Act, the Privacy Act -- I am sorry -- the Delete Act, the California Age-Appropriate Design Code.

The California Privacy Act does cover employees. That might be the only kind of piece that is left since this doesn't cover the employment situation. But all of the provisions in those laws relate to provisions in this bill, so millions of Californians would be left with fewer privacy rights than they have today and that they have had on the books for 8 years now.

In our Federal system, Congress' role should not be stripping privacy rights, eviscerating hard-fought rights that the State legislators have decided they should have.

The Delete Act has been wildly popular. It has only been effective since January 1. I think something like 300,000 Californians have already taken advantage of that, to have that centralized deletion mechanism, because we don't know who data brokers are as consumers.

So it is great that they have one place to go where they can say, "I don't want my information sold by data brokers," and that is conveyed to those companies.

And this would just -- it would leave Californians in a worse place than they are today.

Mr. Mullin. Thank you for that.

I also want to walk through a real world example that our witnesses are familiar with.

Texas recently led a suit against an insurance company that used third-party apps to collect trillions of miles' worth of location data from over 45 million consumers nationwide and used that information to build what has been described as the world's largest driving-behavior database. According to the allegations, insurers then used that data when setting or renewing consumers' insurance premiums.

Under the SECURE Data Act, even if those allegations are true, the company would have

45 days to remedy the issue without any penalty even though the data has already been collected, shared, and sold.

So, Mr. Bridegan, you just mentioned Texas, Texas' biometric privacy law, the recovery of billions of dollars for consumers. As I understand it, that law and others hold bad actors accountability even if they later fix any violations.

However, the SECURE Act would give bad actors 45 days to rectify any violations with no penalty if they do. But fixing the problem going forward doesn't undo the harm that the data has already been collected, already been sold, and consumers can't get it back. So why would we want to preempt State legislation with such a provision?

Mr. Bridegan. Thank you for the question.

I think that case is actually a very fascinating example of how narrow a cure period really is. Texas has a 30-day cure period. That was not curable conduct under Texas' privacy law.

There is actually very few -- we have had to do a lot of thinking on what really is curable. If you collect data about a person without their consent, how do you fix -- you can't really -- how do you cure that?

Do you delete it? I would say you already did the harm by collecting their data without their consent. Deleting it doesn't do it.

If you go back and get their consent, then arguably you still violated that initial provision of the law. There is not really a way to walk that back.

A lot of these data ecosystems are also extremely complex and pursuant to very complex contractual agreements. They are negotiated with sophisticated law firms and parties. Those have mechanisms that can't really be completed in the 30- to 45-day window. You could say you are a counterparty to the agreement, big company, and you sold that data to them, you can't suddenly void that sale of data. And if that company went on and used that data, that would also be another layer of arguably incurable conduct.

I have viewed the cure period as really something that goes for more of the facial violations, so not including the right language in a privacy policy, not having the ability for consumers to exercise their rights working properly. And even that one might get into incurable conduct.

But, ultimately, that case was a very good illustration of sort of how limited the cure period really is ultimately.

Mr. Mullin. Thank you for that. I remain skeptical of the approach before us today.

And with that, I yield back. Thank you all.

Mr. Bilirakis. The gentleman yields back.

I recognize Ms. Lee from the great State of Florida, my fellow Florida Gator.

You are recognized for 5 minutes of questioning.

Ms. Lee. Thank you, Mr. Chairman.

What we are doing here today is so important. Americans should not have to surrender their privacy in order to participate in modern life, and parents should not have to wonder whether a child's personal information is being collected, shared, or sold without their knowledge.

The reality is that technology has changed dramatically, but many of the laws governing how we address personal information have not kept pace.

I have worked, along with many of my colleagues on this committee, to modernize COPA, because the internet children use today looks nothing like the internet that Congress attempted to regulate in 1998.

As we consider a national privacy framework, we should reject the false choice between protecting consumers and promoting innovation. We can do both. And I appreciate all of you for sharing your insight about the pathway toward doing that here today.

States like my home State of Florida have already shown that strong consumer protections and economic growth can go hand in hand. We should build on those lessons by giving families meaningful control over their children's data, strengthening safeguards for sensitive information, and

establishing clear rules that consumers and businesses alike can trust.

Mr. Bridegan, I want to come back to you.

One of the major differences between the SECURE Data Act and some of the existing privacy frameworks that we have been discussing here today is its requirement that companies obtain affirmative consent before processing sensitive information, such as health information, biometric data, or precise geolocation data.

During your time enforcing Texas privacy laws, what types of sensitive data abuses concerned you most? And how does an affirmative consent requirement help us prevent those abuses?

Mr. Bridegan. Thank you for the question, Representative Lee.

When I started heading privacy enforcement for Texas, I did not come in expecting to be focused so heavily on geolocation data. Around that time, The New York Times had reported that several car manufacturers were collecting data from people's vehicles directly and, ultimately, scoring them and sending it on to insurance companies for insurance companies to charge varying rates.

That I think was sort of a novel use in some ways of geolocation data and to me underscores the importance of having a law that has those tried-and-true mechanisms like consent that enforcers can apply to different situations as more data types and uses emerge over time.

A data ecosystem is incredibly complex, but their needs to be enough flexibility and sort of reliance on those mechanisms that we have seen work in the enforcement context. Children's data has emerged and will continue to emerge as an area that requires heightened attention.

Ms. Lee. What is your perspective on the biggest privacy risks facing children and teens today? And how does requiring parental consent help get to ensuring that that minor's personal information can be kept safe and parents can stay in control?

Mr. Bridegan. There is data being collected by children now that I think will stay with them for the next 70 years -- longer. It is unpredictable how that data will ultimately be used throughout

their lives. There has not been enough of a focus on sort of ensuring that going from that age of minority to majority, that there is some sort of clear line about what needs to happen with that data.

On the age-verification front, Texas has been a leader in passing children's online safety and privacy laws. Those all come back to age verification. I know Congress is pushing forward with an additional children's privacy and online safety package, which I think is a great effort because there continues to be sort of a blind spot for parents, an arguably sometimes intentionally blind spot by companies, as to what is happening on these platforms.

Ms. Lee. And do you believe that parental consent in addition to those age verifications plays an important role? And if so, tell us more about that.

Mr. Bridegan. Yes. I think it is key for parents to be in the loop on what is happening, what their children's data is being used for, and what features are allowed for children.

In the social media context there is a lot of -- there was a lot of focus from our office on sort of what different users could -- how they could interact with minors. And there needs to be some sort of stopgap there because there just has not been sort of a required demarcation of preventing certain interactions from adults and minors or minors to minors in several of those spaces.

Ms. Lee. Thank you.

Mr. Chairman, I yield back.

Mr. Bilirakis. I thank the gentlelady.

I will recognize Mr. Veasey for his 5 minutes of questions.

Oh, Ms. Clarke is back. Okay. We will recognize Ms. Clarke.

You are recognized.

Ms. Clarke. Thank you, Mr. Chairman.

And good morning to both you and Ranking Member Schakowsky, my colleagues.

And thank you to our panel of witnesses for joining us today.

Anyone familiar with the work and history of this subcommittee knows that for years I have

been stressing the importance of a comprehensive Federal privacy framework.

While I can appreciate the title of today's hearing, I must address the fact that the legislation before us today is a nonstarter for comprehensive privacy and data security.

In front of us is a piecemeal attempt at protecting Americans online. And to be clear, naming a bill the SECURE Data Act by no means qualifies it as a comprehensive privacy bill. A privacy bill should actually protect privacy.

To level set today's hearing we must acknowledge that my colleagues on the right have not only been unserious about Americans' online safety, they have been actively working against it. Let me remind us all that the party backing this legislation is the same one who has tried to illegally fire the Democratic FCC commissioners, is insistently promoting sweeping preemption of State AI laws, and continues to prioritize big tech over people.

Sorry, but I don't trust this proposal as a good-faith attempt.

It wasn't too long ago that House Democrats and Republicans were able to come together and form the bipartisan AI Task Force that produced a comprehensive report with the intention that it would guide the 119th Congress on the necessary next steps at regulating AI.

My colleagues and I have worked to advocate for the inclusion of civil rights priorities in the bipartisan report. And while it could have gone further, I was proud to see that the task force report emphasized the different biases that AI can hold and how that may affect consequential decisions that AI occasionally is employed to make.

I am beyond disappointed to see that the SECURE Data Act has not only walked back on any effort to protect Americans' civil rights online, but has gone as far as to narrow the scope of protections, water down the definition of consequential decision-making, and preempt State civil rights law.

When Congress works to stymie or dumb down privacy protections and technology safeguards it is working against the public interest. This bill maintains the status quo. Big tech

data brokers will carry on business as usual, collecting and using people's data whether they know it or not.

Now more than ever, we should be holding companies responsible for failing to keep us from harm when we go online, to live up to their promises when they say they care about our privacy, and to hold them to their commitments to ensure that AI systems they create are safe.

I implore my colleagues to recognize that this bill is just not it. This bill will do nothing to prevent or mitigate harm caused when the data collected and used by companies drives discriminatory decisions and will only further harm Black and Brown Americans who will continue to have their data used against them.

I move to enter into the record this letter from the Leadership Conference on Civil and Human Rights into the record.

Mr. Bilirakis. Without objection, so ordered.

[The information follows:]

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

Ms. Clarke. Well, I thank you, Mr. Chairman.

And with that, I yield back.

Mr. Bilirakis. I now recognize Mr. Fulcher, the vice chairman of the subcommittee, for his 5 minutes of questioning.

Mr. Fulcher. Thank you, Mr. Chairman.

The purpose of the SECURE Act is to provide consumers more control over their personal data and create a uniform national framework. The bill does not include a private right of action, and we have seen downsides of litigation abuse in the privacy space in other cases historically.

Currently, opportunistic law firms have filed over 4,600 suits nationwide claiming that ordinary internet activities used in cookies and pixels, bots and analytical tools, constitute wiretapping under various State laws. There have been more than 3,000 of these suits that have been filed just in California alone.

So I am going to just fast forward here, but we have got a situation where one plaintiff has filed 30 lawsuits claiming wiretapping by roofers, plumbers, general contractors, HVAC employees, and so on. Another one has filed 38 lawsuits against Rocket Mortgage, Marriott, HP, Frontier, and Williams Sonoma. There are many more examples like that. But you get the picture of the issue I am trying to bring up here.

A question for Ms. Watts.

In your written testimony you mention that private rights of actions are used to target small businesses who are incentivized to settle cases as opposed to engaging in the costly litigation.

Do you think that if the SECURE Act does not contain Federal preemption that we will see a growth in litigation and privacy suits? And just more generically, what are your thoughts of the ramifications if the SECURE Act did not have Federal preemption?

Ms. Watts. Yeah. Thank you for that question.

I think it is important to note that 22 States have not had private right of action in their legislation. It wasn't even taken out of legislation. It was never included in the first place.

We hear stories from small businesses all the time from other States where they are being targeted by the trial bar, and instead of going through a costly legal system they are settling for $10,000, $15,000 because it is easier to do that than to fight that lengthy court system.

I think it is also important to note that there is recourse in this bill, and, actually, in Kentucky that would be strengthened.

Right now in Kentucky our recourse is to go to our State's attorney general, Russell Coleman, who absolutely has been very communicative with business and with consumers as well on how to, if there is an issue, to complain to his office. He is a former U.S. Attorney and a former FBI agent. He very much wants to protect consumers, and especially children, as has been mentioned throughout this testimony.

I also think it is really important that we make sure that this bill, it is clear that it is not going to protect bad actors.

In addition to States going through their attorney general, there is also the recourse of going to FTC as well. For a State like Kentucky that has passed State law, right now our recourse, kind of our pathway would be to go to the State's attorney general.

Now consumers could go to the attorney general but also the FTC as well. So I think it actually strengthens the protections of the States that already have these bills in place.

Mr. Fulcher. Thank you for that. I appreciate your comments.

Mr. Bridegan, when professional plaintiffs file lawsuits and there is no demonstrable harm, what is the impact of that?

I want to just preface my question by just sharing that I worked in the tech sector before this portion of my life, and as a matter of course, when an officer of a company would sell stock, whether it was in the window of time where that was allowed or not, there would just be a flurry of lawsuits

that got filed automatically. And so there truly are professional plaintiffs out there.

But when those lawsuits are filed and there is no demonstrable harm, what is the impact of that?

Mr. Bridegan. Thank you for the question.

Back in private practice we have had to deal with this a lot. And it comes in waves and I think underscores both the risks of a private right of action, but also the risks of not having a uniform standard.

So using wiretap litigation as an example, that is legal theories crafted by the plaintiffs' bar to essentially claim that someone's privacy rights are violated. It is an unfortunate model where many of them -- and this happens in the ADA website compliance and TCPA litigation as well -- where they will price this opening offer settlement so low that it is more -- but it is more than -- I am sorry. The opening settlement offer is less than what it would take for a company to retain a law firm to respond to the lawsuit.

So they are getting these $5,000, $10,000, $15,000 on behalf of single consumers over and over and over. Oftentimes, several companies will have multiple filed against them in any one time.

It is very distressing for particularly small -- the targets of those are, as Ms. Watts explained it, oftentimes small and medium size businesses that do not have the resources to retain and fight those lawsuits.

Mr. Fulcher. Thank you for that.

Mr. Chairman, I yield back.

Mr. Bilirakis. The gentleman yields back.

I will recognize Mr. Veasey for his 5 minutes of questioning.

Mr. Veasey. Thank you, Mr. Chairman.

Obviously, there are a lot of things about this bill that really worry me. Obviously, we need to do something about data and privacy. I think that everybody agrees on that. But, again, there

is just some worrisome language in this bill.

And I just specifically wanted to ask if Ms. Fitzgerald can answer this question.

I know this bill explicitly bars the FTC from enforcing its own civil rights provision and can only pass complaints to other agencies.

I was wondering that if a company is using personal data to deny someone a ride or a loan or a job based on race, religion, or political views, who exactly is going to enforce that? Because that is what I kind of don't understand.

Ms. Fitzgerald. Yes, that is a very problematic provision in this bill, one of many, and it is unclear who a consumer would go to if they are discriminated against online.

It points to other agencies that the FTC would refer those cases to. But the FTC has historically had that authority to protect consumers when data is used in ways that discriminate against them.

Mr. Veasey. Yeah, that is really interesting.

If a company is caught misusing data to discriminate based on someone's race or religion or politics to give them a job, I know that the bill gives them a 45-day grace period to try and cure exactly what is going on so they can say that it is fixed, no matter how serious the violation may be.

And I was wondering, why is it important for a company to get a free pass just because they promise not to do it again.

Ms. Fitzgerald. Yes. The right to cure in this bill is mandatory. Many States that have included rights to cure have either sunsetted them after a couple of years after the bill comes into effect so that companies have a chance to catch up on compliance for the first couple of years and then it sunsets; or they make the right to cure discretionary so that enforcement authorities can look at a specific case and see that it is curable or decide not to move forward with that if the violation rises to that level.

So I think that those are options that were not included in this bill and that could have been.

And something else that is missing from the SECURE Act is the strong civil rights protections that were included in the American Data Privacy and Protection Act and American Privacy Rights Act that prohibited personal data from being used in ways that discriminate against Americans in many ways.

Mr. Veasey. Yeah. I was wondering from some of the other panelists, does it bother you that there is no language in there to help in those areas of civil rights? Just jump in. I would be curious. I mean, to me this all seems very problematic.

Ms. Goodloe. We agree this is a really important issue, and in the past the Business Software Alliance has called for legislation that addresses AI-related issues, including this one.

We have, though, deferred to Congress on whether to combine that with privacy legislation or to address it through standalone legislation.

We know it is difficult to pass a Federal comprehensive privacy law, and we want to see progress on that. So it is something where we have really looked to leaders in Congress to decide how best to move these issues forward.

Mr. Veasey. Okay. Thank you very much.

Speaking of, that sort of puts the burden on individual consumers to request the deletion of their data, particularly if someone had no idea that their data is being used to profile them and deny services. How would someone be able to make that kind of request on their data?

Yeah, please.

Ms. Fitzgerald. Yes. So companies in their privacy policy are required to explain to consumers how to exercise their privacy rights. So if it is a company that they interact with directly, a social media company or a retailers' website, they would go to the website and either submit a form or email the company to ask to delete their data.

The problem is that there are so many companies that most consumers have never even heard of that are gathering our data every minute of every day, and so they don't have -- they don't know that those companies exist to go to them and ask to delete their data.

Mr. Veasey. Yeah. Yeah.

And my last question. Is it problematic that people will sometimes just click on the box to give people consent? Because I am worried about that. It is almost like when people clicked on boxes before and they didn't know that they were waiving their right to go to trial.

Is that a problem, that people are just basically clicking this box to give consent, a little pop-up box, so they can sort of keep moving along without knowing exactly what they are clicking on? And is that a fair and transparent way to help consumers?

Ms. Fitzgerald. I don't think so, because even if they know what they are agreeing to, there is no choice not to agree. Usually, the proceed button is grayed out until you check the box saying, "I agree to these terms." So that is not a real choice at all.

Mr. Veasey. Thank you very much.

Thank you, Mr. Chairman.

Mr. Fulcher. [Presiding.] Thank you.

The chair recognizes Mr. Goldman for 5 minutes.

Mr. Goldman. Thank you, Mr. Chairman.

First, let me thank my deskmate today, Dr. Joyce. Thank you so much for your leadership on this.

For those of you who don't know, Dr. Joyce and his staff have put an insane amount of hours into this.

And I just want to thank you. It has been an honor to work with you on this.

As a member of the Privacy Working Group, I am proud to cosponsor the SECURE Data Act, which is based on consensus privacy laws like those in my home State of Texas.

Mr. Bridegan, thank you for being here. Great to see a fellow Texan. Thank you for your work on data privacy and security.

If the SECURE Data Act becomes law, would Texas still be able to hold bad actors

accountable?

Mr. Bridegan. Yes. I think, to Ms. Fitzgerald's point, the consent mechanisms, at the end of the day, that shifts the burden to companies to demonstrate to the government. If they can't do that, it is somewhat a sidenote whether the consumer understood or not what was contained in that consent provision. It fundamentally shifts the onus onto companies to be able to demonstrate that to the government.

Compare that to California, which is the only State of every State that has passed a privacy law that does not require consent. This was alluded to earlier, I think Ms. Fitzgerald's point.

In California, by default, as long as a company includes notice of what they are doing with their privacy law, with sensitive data in their privacy policy, they are allowed to collect, use, process, sell, whatever, with that sensitive data.

It is a sort of, I would say, arguably lowest standard for sensitive data of any privacy law in the world at this point. Every other State strengthened that requirement with consent. Some States have taken it further to go to a full-on ban. I would say that even goes further than the GDPR on that front.

Mr. Goldman. Super. And based on your experience leading privacy enforcement in Texas, can you explain why State Attorneys General and the Federal Trade Commission would be better equipped than private trial lawyers to enforce Federal privacy law?

Mr. Bridegan. Yeah. I alluded to this earlier. The wiretap litigation is a really good example of how there is this sort of different interpretation of privacy laws that is inconsistent with, say, take the California wiretap law compared to California's privacy law.

Those provisions, if you comply with California's comprehensive privacy law, that does not immunize you from suit by private plaintiffs. So there are companies that were having to divert resources to -- limited resource dollars for privacy compliance and focusing on these class action private litigation as opposed to implementing requirements that would be required under California's

privacy law.

These laws also give government regulators an immense amount of discretion. If, say, a company doesn't include specific language in a privacy policy, should they now be hauled into court and sued by individual plaintiffs?

I would argue that is not really protecting privacy and taking dollars away from actually making sure compliance programs are up to snuff.

Alternatively, because of the cure period, because these are highly technical laws, those are much more sort of attuned to government interpretation and sort of the injunctive nature that comes along with government enforcement as opposed to a larger focus on obtaining a monetary settlement.

Mr. Goldman. All right. Thank you.

Ms. Watts, thank you very much for coming.

Throughout your testimony you explained that small businesses are increasingly dependant on data technology and online commerce to compete and grow.

Can you explain why the SECURE Data Act is important for the success of many small businesses both in my district in Texas and around the Nation?

Ms. Watts. Yes. Thank you for that question.

As I said, most of our members of the Kentucky Chamber of Commerce are small businesses and they want to grow their businesses. They want to take those businesses outside of the Commonwealth and get consumers and customers from all over the Nation. And so having a patchwork of laws is very cumbersome and burdensome to them.

So really what we have been saying is the 22 States that have these comprehensive data protection laws, really we don't need to reinvent the wheel. We can use what we have done in 22 States that have protected consumers first, but also had businesses have a clear set of guidelines to follow nationwide.

I think it is really important for small businesses in particular to be able to grow their business. And as we know, we are a digital world. I know myself, as a working mom of two, I do most of my shopping on my phone. That is really important to businesses.

We had a small business member that is a member of the U.S. Chamber of Commerce say that if all of the data was gone and all the technology ceased to exist it would be another pandemic for him.

So I think we cannot underestimate the power of technology and data for our small businesses to really grow and flourish like we all want them to do.

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

I do want to thank everyone for being here. It is always great to have a full house and the general public here attending this hearing.

I specifically want to point out we have two young Americans. They have been sitting here on the front row the entire hearing without their phones, without playing games.

I just want to thank you all for being here. You have been paying attention the entire hearing. So thank you all very much for being here especially.

Thank you, Mr. Chairman. I yield back.

Mr. Fulcher. Thank you. We can all take a lesson from that.

The chair now recognizes the Representative from Illinois, Ms. Kelly, please.

Ms. Kelly. Thank you, Chair Bilirakis and Ranking Member Schakowsky, for holding this morning's hearing, and thank you to our witnesses for participating.

As has been said, Americans want a strong privacy act, but the SECURE Data Act does not quite meet the mark and preempts the stronger protections already in place in the States. This piece of legislation keeps a notice-and-consent model in place where a company can collect and use data for almost any purpose as long as it lists that purpose somewhere in a privacy policy.

Almost no one reads those policies. And if you do, cannot reasonably understand them in

many cases. This is not true consent.

Ms. Fitzgerald, you stated that under this legislation a company can bundle a necessary purpose like processing a payment with an unnecessary one like selling data into a single set of terms. When a consumer clicks "accept" do they have any real way to know what they just agreed to?

Ms. Fitzgerald. I think it is difficult for consumers to know. I am a privacy advocate. I still don't read all the privacy policies. You would do nothing else with your time if you read all the privacy policies that you use.

So while consent is an important piece of consumer protection, it shouldn't be the only thing standing between consumers and the collection and use of their data. There should be obligations on companies to limit how much data they are collecting and how they are using it. Because if the only protection is at the end of a long privacy policy there is a checkbox for "accept" and I have to check it in order to use the website or app, that is not a meaningful protection. That leaves me with no choice. In modern day society there are just so many apps that we have to use.

Also, I want to highlight that there are protections in many State laws in terms of what consent means that were not included in this bill, the protections that Mr. Bridegan mentioned about making sure that consent isn't just acceptance of broad terms and conditions.

Or prohibitions on dark patterns. There is nothing in this bill prohibiting dark patterns. So that means that a company can just have one big, brightly colored "accept" button and then "disagree" in small fonts and requires toggling a dozen buttons.

So you want to make sure that when you are using consent it is meaningful and that it is not the only protection for consumers.

Ms. Kelly. Thank you.

Ms. Goodloe, your members write the privacy policies in consent screens consumers use every day and your testimony says that Federal law should help people trust their data is used

responsibly. That trust depends on people understanding what they agree to.

What standard would your members support to make sure consumers actually understand what they are agreeing to?

Ms. Goodloe. Thank you for the question.

And before I respond, I want to clarify, I represent the business-to-business part of the technology industry. I know we have talked about the technology industry more broadly. I represent BSA members who are a very specific part, providing business-to-business technologies to companies of all sizes across every industry sector, things like cloud computing, software that can track inventory and keep track of customer service inquiries, the sort of back-end functions that everyday businesses across the economy rely on.

Very often it is those other companies, the consumer-facing companies, who are creating the sort of privacy policies to tell consumers what they are going to collect from the consumer, how they are going to use that information.

I think the bill that is before this committee today reflects both of those roles by being anchored in this longstanding distinction between controllers who decide how and why to collect data and processors who handle it on their behalf.

When we step back and look at the consent requirements that apply to those controllers, the ones who are deciding, "Why do I collect a consumer's data, how am I going to use it?" I think that is a longstanding and very important topic in the broader conversation about privacy legislation and the right set of safeguards on how companies collect and use consumers' data.

And I think there has been a concern that consumers are sort of bombarded by consent requests and it ends up in a situation where they are unable to read all of them.

At the same time, consent is an important guardrail and consumers do want to know when companies are collecting very sensitive types of data and know how companies intend to use that data and be offered that choice.

This bill requires consent to collect sensitive data. As some of the other witnesses have mentioned, that is stronger than the law right now in California. But I think the goal of privacy legislation is to make sure that that consent is meaningful and consumers actually have a choice about the things that matter most to them.

Ms. Kelly. Thank you so much.

And thank you to all the witnesses.

I yield back.

Mr. Fulcher. Thank you.

And the chair recognizes Representative Fry for 5 minutes please.

Mr. Fry. Thank you, Mr. Chairman.

You know, I found myself in this working group just kind of really interested in diving into the legalese of what States are doing, how they operate, the lessons learned.

I served in the State Legislature and we often borrowed good ideas from other States and we shunned ones that were not successful in other States. And this is I think no different when you are looking at this.

Ms. Watts, what do you think is important here? What are the competing interests that exist when you were debating this in the Kentucky Legislature?

It seems to me that the competing interests are privacy, citizens' right to their data maybe, but also innovation, small business entrepreneurship. That seems to be kind of the rub, right, between the two sides? Is that fair to say, roughly?

Ms. Watts. Yeah. Thank you, Representative Fry, for that question.

We passed this bill back in 2024, and you, as a former State legislator, I know that sometimes it does take a couple years to get the right bill. We worked for several years with a broad coalition.

And I often say I know many of you work with your local or State chambers of commerce. If the chamber of commerce had one superpower it is the ability to convene and find consensus. We

bring groups of all different shapes and sizes and sectors to the table to really find a feasible path forward, and that is exactly what we did with House Bill 15 back in 2024.

Mr. Fry. So you guys, you worked with stakeholders with different ideas on what is acceptable and what is unacceptable, and they were not always aligned. Is that correct?

Ms. Watts. That is correct. I mean, I said earlier, I have been doing this job for 14 years, and very rarely have I ever passed a bill unanimously through the Kentucky General Assembly, but this was one of them. So you are exactly right. It was the balance of consumer protection but also business innovation, making sure businesses can flourish.

Mr. Fry. Isn't that the balance that we have right now, Ms. Goodloe, right? I mean, to your point, you have multiple States that have done this. California's model seems to be modeled after the European model more than it does some other States. Would you characterize it that way, Ms. Goodloe?

Ms. Goodloe. Thank you for the question.

I think California has a different approach than the other 21 State consumer privacy laws, and California took the important step of adopting the United States' first State-level comprehensive privacy law back in 2018, but we haven't seen anyone copy it since.

The model that has been widespread throughout the States where it had common agreement is this model that has a core set of rights, a core set of obligations for companies, to make sure that their data is used responsibly, and it is regulatory-led enforcement. And that is the model that we see in the SECURE Data Act.

Mr. Fry. Do you know what happened in Europe after they passed the GDPR model, what happened to investment in Europe in tech? Do you know?

Ms. Watts, would you care to guess?

Ms. Watts. Yeah, I would like to comment on that.

Recently, the European Commission has said that the overregulation has harmed their

economy, and when every day we talk to our consumers, our businesses about affordability, I do think it is a great concern to be going down the path of what Europe did with privacy.

Mr. Fry. Yeah, in fact, the National Bureau of Economic Research found that the GDPR took -- it took effect in 2018, has seen technology startups decline in Europe.

And so when we talk about competing interests, when we talk about this in a global economy that we have, what Europe did might have been an overreaction to a problem, and maybe what California did was an overreaction to a problem.

So States like Kentucky seem to be trying to find the right balance. Is that fair to say?

Ms. Watts. I think it is absolutely fair to say. And like Ms. Goodloe said, I think it is very important to note that California -- no other States have passed the California model. We are pretty proud that many States have passed the Kentucky model or the Virginia model.

Mr. Fry. They were first, but everyone said we don't want any part of that, we don't want that.

Ms. Watts. It doesn't work for business. It doesn't balance those rights of consumers --

Mr. Fry. Correct.

Ms. Watts. -- as well as let business flourish and innovate, which is what we want them to do.

Mr. Fry. Ms. Watts, why do you think it is important that this bill, the Federal bill, have a strong preemption on privacy laws?

Ms. Watts. I think it is important so that businesses know what rules to follow. And like we have mentioned before, large businesses have teams of attorneys and privacy officers and they can usually navigate the complexity of various State laws.

I represent mostly small businesses who do not have that. They are dealing with workforce issues, with inflation and affordability and all the things that small businesses deal with every single day.

Mr. Fry. So if you are a big, big tech company, you have got the lawyers to be able to navigate a 50-State patchwork of laws, right?

Ms. Watts. Yeah, of course.

Mr. Fry. If you and I decided to put 100 bucks into the collection plate and start up our own tech company, would we have those same financial resources to navigate 50 State laws?

Ms. Watts. Absolutely not.

Mr. Fry. So we stifle innovation if we don't do something about this.

Ms. Watts. Correct.

Mr. Fry. Thank you for that.

Mr. Chairman, I yield back.

Mr. Fulcher. Thank you.

The chair recognizes the gentlelady from Washington, Ms. Schrier please.

Ms. Schrier. Thank you, Mr. Chairman.

Congress has talked for years about passing comprehensive privacy legislation to give consumers the ability to keep their data private and secure. And so I am really glad we are holding this hearing today to discuss policy that we are long overdue in passing. And I appreciate all of your comments.

The internet basically runs on your data. There is the old adage: If something is free, then you are the product. And I think we should all keep that in mind. Just about every app, every site, every interaction online is collecting personal data that companies can use and sell to their financial benefit, and not necessarily or not at all comparably to yours.

And it is almost impossible to track exactly when your data is being collected and certainly impossible to track where it goes afterwards and for what purpose, who is getting ahold of it. And that is why an enforceable right to privacy is so important.

But a national standard, although I understand the importance of preemption, it is useless if it

is weak and it doesn't actually give consumers control over their own data. And, in fact, a national standard can be actually actively harmful if it overrides or fails to adequately replace the protections that have been passed already in dozens of States.

That would certainly be true for Washington State, which passed the My Health My Data Act into law in 2023, and this law protects Washington residents' health data beyond the limits of HIPAA.

HIPAA protects patients by preventing healthcare providers from sharing or selling your data, but it doesn't prevent other companies from tracking, analyzing, selling your health data that they collect in other ways.

Like HIPAA doesn't cover health tracking apps or wearable devices that are collecting unprecedented amounts of your biometric data. It doesn't cover companies using your data to infer health conditions from your purchasing history.

I think we all remember people getting advertisements for cribs when they started buying prenatal vitamins at a certain large retailer.

But the My Health My Data Act does, and it has been an enormous step toward giving Washington residents privacy when it comes to their health. It has strict data-minimization standards and ensures that companies have to gain explicit authorization to collect and sell personal health data.

And specifically that authorization cannot be part of a broad terms of use agreement or through any kind of hidden or deceptive means. So that means it can't be buried in a long legalistic notice that no one ever reads or hidden behind a complicated menu of options.

But the SECURE Data Act would override this State law, and its health protections are not nearly as robust as Washington State's. So I fear this would be a net loss for my constituents and this would happen in a patchwork of States across the country.

Ms. Fitzgerald, thank you for all of your comments. Can you speak to the kinds of robust protections and data-minimization standards that you would like to see for health data specifically?

Ms. Fitzgerald. Yes. Thank you for the question.

There was just a discussion of whether GDPR and California overreacted to the problem. I think it is important that we also don't underreact to the problem.

People are being harmed by these data practices every minute of every day and health data is a really good example of that. So any Federal privacy law should require that the companies collecting that data limit it to what is necessary, line it up with what the consumers expect, and then make sure not only that the collection is limited, but also those uses, because often it is the secondary uses of our data where the harm is really happening.

We expect our fitness tracker to collect our health data and provide those services, but if they are selling it to third parties, that is where the harm really, really happens.

Ms. Schrier. That is right. And we have seen this with the ability to get life insurance, health insurance, the ability to get car insurance when our data gets sold without our authorization.

Something that concerns me about the SECURE Data Act is that it places so much of the burden on consumers to navigate all these different opt-out options to protect their data, and the functionality and the ease of use is really going to make the difference here. I think more burden should be put on the companies that have been profiting off this data to protect this data.

And I really appreciate that the bill commissions a study on universal opt-out mechanisms. But I think we need to take more action than just a study. And the reality is that Congress is playing catch-up right now to the States. I am glad we are having this discussion.

But as, Ms. Fitzgerald, you noted, in 2022 we had a stronger bill, and I think it is time to return to that. We can do better. We should do better.

And I yield back.

Mr. Fulcher. Thank you.

The chair recognizes Representative Cammack for 5 minutes please.

Mrs. Cammack. Thank you, Mr. Chairman.

Thank you to our witnesses and all our guests here today. It is nice to see the committee room packed full.

I am going to start with you, Ms. Goodloe. In your testimony you state that the SECURE Data Act reflects the modern economy by recognizing different roles and responsibilities with respect to data, especially differences between controllers and processors.

Can you discuss how the SECURE Data Act distinguishes between these roles and responsibilities, why it is important to do so, and for folks watching at home, the difference between the two?

Ms. Goodloe. Yes. Thank you very much for the question.

This is a core issue for our members who are the business-to-business technology providers that are competing to provide privacy protective and security protective services to other companies.

The distinction between controllers and processors is longstanding, widespread, found in every State privacy law, and it underpins modern privacy laws worldwide.

It matters because if you conflate controllers and processors you end up creating privacy risks for consumers. It is important to know that controllers are the companies that decide how and why to use a consumer's data. Processors are the companies that handle that data on behalf of another company.

So one example is, if you join a gym and the gym keeps your data in the cloud, because it is not going to keep it in a file cabinet, the gym is deciding how to collect your data, why it is going to use that data, and it is giving it to the cloud storage company to handle it as the gym says, on its behalf.

RPTR KERR

EDTR ROSEN

[12:14 p.m.]

Ms. Goodloe. So the cloud storage company is a processor here.

If we conflate these roles and the privacy law starts assigning the wrong obligations to the wrong type of company, what we have seen is it can require that cloud storage company to start looking at all the membership data the gym stores with it, and we don't want that.

The goal of a privacy law should be to minimize how companies review data and not require them to start looking at data that they otherwise would not. That can happen when we conflate these roles. That really goes against the goal of privacy legislation.

Mrs. Cammack. Excellent. Thank you for that. That is a perfect dovetail into my next question. So I am going to start with -- I am a very proud Floridian. Go Gators! I am proud to represent the real gator nation, and so many people on this committee know that I am always talking about my gators.

So I am very pleased that this legislation, the SECURE Data Act, is building on existing State privacy and data security frameworks like those that we have across the country, but in particular, the sunshine State. So less than half the country has comprehensive privacy laws in place, and I believe that every American should benefit from the rights and protections that Floridians enjoy every day.

So I am going to start with you. I am going to mess up your last name. So I am going to try really hard. Bridegan?

Mr. Bridegan. Close enough.

Mrs. Cammack. Sorry.

Can you share more about the consumer protections and rights that are laid out in the SECURE Data Act, and why it is important that we have a uniform Federal framework?

Mr. Bridegan. Yes. I think the data minimization point is a really interesting one. Harkening back to the consent piece that we have been talking about, because of consent, although it is somewhat of an amorphous standard, we know what it doesn't look like. We had some great examples of it does not look like that disclosure at the end of a privacy policy that requires the click of a box.

Again, consent interacts with data minimization in a really interesting way, which we saw from the enforcement lens. Data minimization is somewhat not needed for sensitive data because you have to have consent unless the company is actively able to get that consent. If they collected that data without that consent, they are in violation of the law. It doesn't matter whether they needed it or not.

So that is a sort of point to just to keep in mind, that these provisions are all interacting with each other.

Also, data minimization is a, frankly, more difficult provision to enforce. It is also a somewhat amorphous standard. Sometimes, harkening back to consent again -- if someone violated the consent provisions, I would rely on that as an enforcer to point to that they violated the law. I would not necessarily need to.

I could add on a violation of data minimization, which is what California recently did. Because California does not have consent protections for sensitive data, in a recent settlement with a vehicle manufacturer a couple of weeks ago, they had to rely on their data minimization violation.

Mrs. Cammack. And I know you want to finish that thought. So I am going to ask you to finish that thought in writing because I want to do a quick rapid fire across the whole panel.

When we are talking about data and data privacy, when it comes to a consumer, should they have the option to opt in or out when they are signing up for a service? And I am just going to start with you, and we will go down the line. Opt in or opt out?

Mr. Bridegan. For both sensitive and nonsensitive?

Mrs. Cammack. Let's just go broadly and say nonsensitive.

Mr. Bridegan. Nonsensitive? That would be an opt out.

Mrs. Cammack. Okay.

Ms. Fitzgerald. The company should have to limit what they are collecting and using. It shouldn't all be on the consumer.

Mrs. Cammack. So they should be forced to -- so consumers should opt in?

Ms. Fitzgerald. They should not be presented with constant pop-ups that will make their internet experience unusable.

Ms. Watts. In Kentucky, we would opt in.

Ms. Goodloe. For nonsensitive data, I think opt out has been the standard, in part, to avoid having too many consent requests going to consumers.

Mrs. Cammack. Okay. I am going to say, Ms. Watts, I am with you on this one. I think there should be a blatant opt in, in order for people's data to be shared.

I have a final question. I will submit it for the record. I appreciate your prompt responses. Thank you.

I yield.

Mr. Fulcher. Thank you.

The chair now recognizes the gentleman from Florida, please, Mr. Soto, for 5 minutes.

Mr. Soto. Thank you, Mr. Chairman.

You know, Americans are desperate to take back our privacy rights. For generations, people conducted transactions without a trail of their personal data left behind. Imagine when I was a kid going to major retail stores or to the mall or all these other places, and they didn't get your biometric data. They didn't get your religion. They didn't get so many different things that now we have to protect.

But now that we are online, every transaction leaves a long trail of breadcrumbs, and it has

fundamentally changed the dynamic between consumers and businesses.

Americans want to own their own personal data. We want more control over it. We want to protect it from misuse. That is why we have so many people here today sharing those same values, and we especially want to protect our kids.

The personal data that is recognized as sensitive is a good list. I do agree with it. Health and DNA data, geolocation, calendar, children's data, religion, immigration status, ethnicity, and others, these are things that people should be able to protect if they want to. Yet, the enforcement is lacking. Rules without a strong enforcement is like a tiger without teeth.

No cause of action means we can't have strong -- we can't have a strong cause of action without -- we need a strong cause of action and preemption together that is reasonable. If you do one without the other, you could actually have really unintended consequences.

So if you have strong preemption but then you block State causes of action, and you have no Federal relief, then you have actually just shut the door on a lot of these States we have heard from, both Kentucky and Texas today, on their regimes that they have.

And then when you look at what the FTC can do, they really can't take meaningful action in this bill. They can't address civil rights issues or protect personal data. They can refer it to attorney generals, and this is where I get deeply concerned about the bill. If you leave this all with the State attorney generals, you are going to have different enforcement by different attorney generals by how aggressive they want to be and how much they want to deal with thousands and thousands of complaints. So you go from a patchwork of laws in the States to a patchwork of enforcement depending on what the attorney general wants to do.

Now, I know a lot of States that have done these privacy laws but have not included a private cause of action. My own State of Florida, although there are three common law privacy laws that you can make, like appropriation, intrusion, and public disclosure of private facts, but I notice Kentucky and Texas has no cause of action either, right.

So we are giving a lot of work to the State attorney generals, and I worry whether they are going to be equipped to handle this kind of volume. In my opinion, we at least have to have injunctive relief and attorney's fees available so that most people can't afford to hire an attorney just to do some personal data violation that they have. And you need to make sure you can take down the information that you want to take down.

So we can argue about anything beyond that, about proper compensation, whether we have it or not, but injunctive relief and the ability to make sure you can hire an attorney is absolutely critical if we are going to have strong preemption provisions on the Federal level. And I get it. This is interstate commerce if the internet is flowing through different States.

So first, Ms. Fitzgerald, what happens when consumers face violations of the privacy but they can't go to court to fix it? What is traditionally -- what are you seeing across the States right now? How quickly can they get their data offline?

Ms. Fitzgerald. Yes, unfortunately, without a private right of action, there is little they can do, and I think, you know, it is really important when we are talking about a private right of action to recognize that it is not an all-or-nothing proposition. You know, we can talk about small business carveouts for a private right of action.

The bipartisan bill that passed this committee on a vote of 53:2 included a compromised private right of action that focused on injunctive relief and actual damages to avoid some of the issues that were raised earlier. So, you know, I think if both sides come to the table, and we can come up with a compromise, there are ways where individuals would have the ability to enforce their privacy rights, as opposed to, you know, what is in this bill right now, which is they are left without a remedy.

Mr. Soto. I am glad you mentioned the small business exception. We are not talking about someone with one little website that makes a mistake at one of your local barber shops or general stores or other restaurants or retail establishments. So where do you think this small business

exception should fit in because that is very important?

Ms. Fitzgerald. Yes, States have been considering private rights of action. You know, it has struggled to get across the finish line, but one option is set a revenue threshold or set a threshold of companies that only collect over X amount of personal data and only have the private right of action apply to them. Because as you mentioned, State attorney generals are underresourced, overworked. And if you are talking about cases against some of the biggest companies in the world, and they have two or three assistant attorney generals in a privacy division, you are talking about 5 years of those people's time, and that is going to be, you know, taking up their entire workload --

Mr. Fulcher. The time has expired. Thank you.

The chair recognizes the gentleman from Ohio, Mr. Balderson, for 5 minutes, please.

Mr. Balderson. Thank you, Mr. Chairman, and thank you all for being here today.

My first question is for Ms. Watts. Good afternoon. Last Congress, this committee considered data processing rules or data minimization standards that were equivalent to Europe's burdensome general data protection regulation. According to economic analysis, if the U.S. were to adopt European style data standards like some are proposing, it could cost the U.S. up to $123 billion and cost up to 340,000 jobs.

Can you discuss the impact that strict European style data standards would have on businesses, especially small and Main Street?

Ms. Watts. Absolutely. Thank you for that question. Representing small businesses in Kentucky, which, obviously, borders your great State, we are really proud to make sure to protect small businesses in our State law in Kentucky. We know the European Commission has now said that overregulation has actually harmed their economy.

And I know much like you, which borders our State, we are dealing with affordability and the cost of small business to just keep their businesses open every day, and we really can't risk that. So we definitely do not need to go down the path of having the European style model that they have

now been on record saying the overburdensome regulations have harmed their economy. You quoted it yourself. It could cost up to 340,000 jobs. We absolutely do not need that in the United States.

Mr. Balderson. Thank you very much, Ms. Watts. I appreciate that answer. And we love Kentucky, Ohioans do.

My next question is for Mr. Bridegan. Thank you for being here, sir, also. Some advocates argue that these European style data standards are necessary to protect consumers. In your opinion, as a former privacy and technology enforcement official, what effects would adopting those stricter European style rules have on consumers and their privacy?

Mr. Bridegan. As I alluded to in my opening, we have now learned a lot about emerging privacy harms and which protections actually can help consumers and help regulators to go after those privacy harms and which can't, including additional language in a privacy policy that is prescriptive. There is not necessarily any tangible benefit because the consumer and all of us don't tend to read those privacy policies. So there is a balance that I think needs to be struck of what is prescriptive in the sense that it is actually getting to those core privacy harms.

And I have harped a lot about sensitive data. That is just one category. That is an area where there needs to be heightened protections. We have seen that on a bipartisan basis. Illinois, Washington, Texas all have heightened data standards for sensitive data types, and several of them have standalone privacy laws for just those sensitive data types.

So it is important to keep in mind and really think through which requirements are actually protecting consumers from privacy harms. I think California has a long list of -- a long law, a lot of regulations that I would struggle to see how a violation of many of those actually resulted in a tangible privacy harm.

Mr. Balderson. Thank you very much for that detailed answer. I appreciate that.

My next question is for Ms. Goodloe. Thank you for being here, ma'am. Small businesses

that sell products online may interact with customers in all 50 States even though they are often run out of a single storefront or a garage. How does the existing patchwork of privacy requirements complicate day-to-day operations for those businesses? And I will have a follow-up for you.

Ms. Goodloe. Thank you for the question. Right now, companies are required to track 50 moving goalposts to do business in the United States. As long as they are serving customers in more than one State, they need to keep track not only of the 22 States that have already enacted laws, but of the many States that are already revising and amending those laws, and by my count, we are up to 30 amendments.

We need a clear national standard that sets one set of rules so that companies can operate nationwide and know how to protect consumers' privacy.

Mr. Balderson. Thank you.

My follow-up then, and we have about 1 minute left, in contrast, how would establishing a single national standard under the SECURE Data Act make it easier for them to serve customers across State lines?

Ms. Goodloe. I think it tells them what to do. Our companies, as business-to-business technology providers, are in the business of competing to provide privacy protective and security protective services. They want to comply with strong privacy laws because their customers demand it. When they know the rules, when there is a single, clear rule and regulatory-led enforcement, it helps them know what to do to focus on core protections for consumers, and providing one standard can do that.

Mr. Balderson. Thank you very much.

Mr. Chairman, I yield back.

Mr. Fulcher. Thank you.

The Chair recognizes Representative Trahan for 5 minutes.

Mrs. Trahan. Thank you, Mr. Chair, and I want to thank the panel as well.

You know, Federal consumer privacy law is certainly long overdue. There is broad agreement on that, but I do worry that this Congress is going to again fail to make progress on it. I appreciate Representative Joyce and the committee's work on the SECURE Data Act, but I am concerned that it falls short in a few ways, and I am going to use my time to identify one of them, and that is the unique harms that data brokers perpetuate and advanced artificial intelligence exacerbates.

Today, AI can be used to correlate data from across datasets. Meaning anyone with access to an AI model can purchase your data from a broker and paint a very intimate picture of your life. From your location, to your browsing data, and your purchases, bad actors can infer your sexual orientation, how much money you earn, and where you work, study, or worship.

Ms. Fitzgerald, how can AI now draw these kinds of inferences about people who never knew that their data was collected and never consented to it? And what are the privacy risks of advanced AI systems built on data acquired from data brokers?

Ms. Fitzgerald. Yes, thank you for that question. AI is turbocharging the ability for companies to make inferences about consumers, and that is leading to data discrimination. And, you know, surveillance pricing is another harm that consumers really can't stand that is being turbocharged by AI. And strong data privacy legislation is a really critical baseline protection to protect Americans from the harms of AI. It doesn't do everything, but it is a really important first step.

Mrs. Trahan. Thank you.

As you mentioned, it is so critical that data privacy legislation provide Americans a meaningful way to prevent their data from being collected, stored, or sold by data brokers. While the bill requires data brokers to allow Americans to opt out, this must be repeated for every data broker, meaning that you might have to opt out of hundreds, if not thousands of times.

I have a bill, the DELETE Act, which would give Americans control over their own data by

allowing them to force data brokers to delete their data and stop collecting future data through a single opt out request. So, Ms. Fitzgerald, would a single, universal opt out be more effective for consumers than requiring them to opt out broker by broker?

Ms. Fitzgerald. Yes. A centralized dilution (ph) mechanism is especially important when we are talking about data brokers because these are companies that consumers don't know have their data, don't even know exist for the most part. I don't think many Americans could name a data broker for you, and they have never interacted with these companies. So they don't know who to go to, to ask to delete their data.

So the centralized solution mechanism is really important. There is a reason it has been incredibly popular in California. In just the 5 months since it went into effect, 300,000 Californians have taken advantage of it, and I think that shows the desire Americans have to protect their information from data brokers.

Mrs. Trahan. But even the universal opt out has a loophole here. The bill bars Americans from requesting deletion of what it calls de-identified data. Brokers can keep collecting and selling it so long as buyers promise not to reidentify it. So have there been cases before where de-identified or pseudonymous data was able to be linked back to individuals? And what kind of information might bad actors be able to infer even from de-identified data?

Ms. Fitzgerald. Thank you for that question because it highlights something that hasn't been raised yet today.

There is an exemption in this bill for de-identified and pseudonymous data, as you mentioned, and pseudonymous data in particular is problematic because it includes things like our advertising ID and our IP address. These are identifiers that companies are using to track us across the internet, and by exempting them from the consumer rights in this bill, exempting them from the opt out, it almost makes the opt out meaningless because they are not often identifying it with my name. They are identifying it with my advertising ID.

So the FTC has long-held the position that pseudonymous identifiers, it does not render data anonymous. So that is not something that should be exempted. And then in the case of de-identified data, yes, there have been many cases where de-identified data has been able to be reidentified back to the original consumer.

Mrs. Trahan. Thank you.

Look, I believe there is agreement across the aisle that Congress must act to protect Americans' privacy, as a number of States have already done. The recent advancements with AI make this issue even more urgent, but this bill, as written, fails to meet the moment.

So I look forward to working with my colleagues, and I yield back. Thank you.

Mr. Fulcher. Thank you.

The chair recognizes the gentleman from Colorado, Mr. Evans, please, for 5 minutes.

Mr. Evans. Thank you, Chair, and, of course, to the ranking member for this hearing and to the witnesses for coming today.

Strong data security is essential for protecting consumers in today's digital economy. The FBI's internet crime complaint center showed that consumers lost more than $20 billion in fraud just last year. In Colorado, there was a total financial loss of $355 million statewide, and that is an increase of more than 250 percent since 2020.

Colorado has got one of the fastest aging populations in the Nation, and we see scammers and fraudsters are explicitly targeting seniors with complex schemes and phishing traps. I saw it during the 10 years that I spent as a cop in the Denver metro area, and, unfortunately, Colorado has the third worst rate in the Nation for senior fraud. We have got malicious cyber actors, weak data security.

These are some of the reasons that Americans are facing a fraud epidemic, and it is why I am pleased to see the SECURE Data Act requiring companies to adopt some commonsense data security measures to protect constituents like mine from these fraud impacts.

And so, Ms. Goodloe, first question to you. Since you are here from the Business Software Alliance, can you share how the SECURE Data Act's data security requirements work in practice and how the industry can integrate them with existing policies?

Ms. Goodloe. Yes. Thank you for the question. I think this is a very important issue when we think about privacy legislation.

The SECURE Data Act requires controllers to adopt reasonable security measures to make sure that data is kept secure and confidential. What that means in practice is that companies have to establish, implement, and maintain data security practices, and we see this requirement already across State laws, and it needs to apply nationwide.

The SECURE Data Act also tells companies how to do this because it creates a rebuttable presumption that they satisfy this obligation if they use leading tools like cybersecurity risk management frameworks that have set the gold standard globally.

Mr. Evans. Thank you so much.

The next question will be to Mr. Bridegan. We know prevention is the first step in making sure that people's data stays safe from fraud and from these malicious actors, but we still need to be able to go and prosecute the bad guys because they sit around all day long and try to figure out how to hack and bypass these security protocols. You know, security isn't static.

So when you have malicious actors that still work overtime to go out and do bad things, defraud Americans, we have got to have the ability to go get those guys. So I am pleased to see that the National Insurance Crime Bureau has sent a letter supporting the SECURE Data Act because this helps us not only detect, prevent, and deter insurance fraud and financial crimes and related crimes; it also helps us work with law enforcement to be able to go and get the bad guys.

So can you talk a little bit about how the SECURE Data Act works with law enforcement to protect Americans?

Mr. Bridegan. Yes. I think, in general, the more cyber requirements that companies are

required to implement, the greater the chance that law enforcement can do its job. Because the more protections you have on the front end, you are collecting more information about those threat actors, and ultimately, you can coordinate with law enforcement to help go after them.

We recently recovered on behalf of a client, a financial institution that was defrauded, a six figure amount, go after the fraudsters civilly because of our work with law enforcement who was able to go after them criminally. So it is an incredibly complex scheme, but it is permeating throughout the United States, as you alluded to.

Mr. Evans. And then my final question, and this is, unfortunately, just a tragically horrifying statistic. Colorado has got 2 percent of the Nation's population, but we are 10 percent of the human trafficking in the Nation, and a lot of these are kids that are being subject to this. And we know that when you have human trafficking, there is money transactions. There is a lot of digital footprint that is involved here.

So, again, we want data privacy for Americans, but we also have to be able to interrupt not just the financial crime space, but we have to be able to trace that back and untangle that to horrific crimes like human trafficking and human trafficking of minors.

So can you talk in my remaining 30 seconds just a little bit about how this not only works to protect Americans' data and to work with law enforcement not just on the financial piece but also on things like human trafficking?

Mr. Bridegan. Yes. Again, this bill helps create that information flow between law enforcement and the private sector. The FBI has done a great job over the past decade or so holding itself out as a partner to companies that are, you know, either observing crime or the target of fraud. And so there has been that palpable shift over the past decade to really encourage that coordination, which I think is so key to getting at the core issues here.

Mr. Evans. Thank you so much. I am out of time. I yield back.

Mr. Fulcher. Thank you.

The chair recognizes the ranking member for 1 minute, please, Ms. Schakowsky.

Ms. Schakowsky. I am concerned that this bill right now protects companies and not people and that what we really need to do is protect our everyday people, and that is not happening right now.

Mr. Fulcher. Thank you.

The chair recognizes the gentleman from Ohio, Mr. Joyce, for 5 minutes.

Mr. Joyce. From Pennsylvania, the other Joyce, but it is good to be with you.

Mr. Fulcher. My apologies about that.

Mr. Joyce. Thank you.

Thank you for our witnesses for being here. Thank you for participating in this candid conversation.

To start, I would like to rebut a shallow attack on the SECURE Data Act, that the SECURE Data Act's consensus approach is flawed because it is based on over 20 States, blue, red, and purple States. To that end, Mr. Chairman, I would like to enter into the record a May 11, 2022, press release from the well-known consumer advocacy group consumer reports that is entitled "Connecticut governor signs comprehensive bill into law that explicitly states this year we saw giant tech companies push weak bills at the State level. So we are especially pleased to see Connecticut sign a strong law that will extend real privacy protections to its citizens."

In May 2022, a Connecticut law that was modeled on Virginia, modeled on Colorado, and modeled on Utah laws was dubbed by consumer advocates as extending real privacy protections, protections to consumers and not the product of giant tech companies.

Yet today, a Federal law that is modeled and centered on those exact laws and extends privacy protections to all Americans is somehow, in retrospect, all just part of some multiyear, multidimensional scheme by Big Tech to ultimately create a Federal standard. This is a clear example of how consumer groups will move the goalpost not based on what is working for the

consumers, but rather, on a desire to hamper legitimate uses of data that benefit American consumers and American workers.

For far too long, consensus on Federal privacy reform has been elusive, and a lack of that consensus has plagued legislation in multiple Congresses. As I shared at the beginning of this hearing, hours ago, I am committed to working with my colleagues on both sides of the aisle, as well as stakeholders, to advance the strongest possible bill out of this committee and onto the House floor.

Ms. Watts, why do you believe that the consensus State approach to comprehensive privacy and data security offers the best pathway forward to consensus from the Federal level?

Ms. Watts. Yes, thank you for that question. Thank you for all of your work on this bill. We are really proud in Kentucky to have had a consensus-based bill that passed unanimously through our general assembly and was signed into law.

Mr. Joyce. How is it working?

Ms. Watts. It is working great so far. It just went into effect in January, so passed during the general assembly of 2024. It is now in full effect. We actually just checked with our attorney general --

Mr. Joyce. You worked hard to get that passed.

Ms. Watts. We worked very hard, and I will say for a couple of years, we really wanted a Federal bill. We wanted you all to take that step so that there was not going to be a patchwork --

Mr. Joyce. This passed unanimously, you said, earlier?

Ms. Watts. It passed unanimously, and we are a super majority --

Mr. Joyce. A super majority of which side?

Ms. Watts. Republicans.

Mr. Joyce. And who signed it into law, a --

Ms. Watts. Democratic governor, Andy Beshear.

Mr. Joyce. And this shows that this is a bipartisan concern --

Ms. Watts. Completely.

Mr. Joyce. -- and we in the U.S. House of Representatives understand that and can work in a bipartisan manner to make this effective.

Ms. Goodloe, can you please talk to us about comprehensive privacy and data legislation from a whole economy regulation? Because you deal business-to-business, and you understand the entire economy from the tech sector, and the SECURE Data Act will grant consumer rights and protections across all industries, from life sciences to real estate to manufacturing.

Talk to me how that will affect that business-to-business relationship.

Ms. Goodloe. Well, I should start by saying thank you for all of your work with our working group to work on pushing forward comprehensive Federal privacy legislation. We deeply appreciate that because this matters to BSA member companies. We have long supported Federal comprehensive privacy legislation because it is important to the national economy. Companies of all sizes and in all industries rely on technology.

BSA represents the business-to-business technology providers that power businesses in every sector, and so what we see is a need for a single standard that sets the right level of consumer protections for companies nationwide and across sectors.

Mr. Joyce. That U.S. digital economy that supports all sectors supports over 28 million American jobs, which means that the stakes are serious for so many Americans. We need to get privacy right, and we have seen in Europe that embracing impractical and burdensome approaches to privacy results in stagnation and results in job losses.

The SECURE Data Act is a result of a consensus framework. I think it was Justice Brandeis who said 80 or 90 years ago that the States are the laboratories of democracy. We took that very seriously. We looked at the 20 plus States that have privacy acts. This is our opportunity to bring consensus-based legislation that protects consumers, first and foremost, and gives certainty to

American businesses to stop moving the goalpost.

Once again, I look forward to working with all of my colleagues on both sides of the aisle to advance the SECURE Data Act. Again, I thank you for being here with us on this long morning, and, Mr. Chairman, I yield back.

Mr. Fulcher. Thank you. And the chairman appreciates the good gentleman from Pennsylvania.

I ask unanimous consent that the documents and the staff document list be submitted for the record. Without objection, so ordered.

[The information follows:]

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

Mr. Fulcher. I would like to thank our witnesses for being here today. Members may have additional written questions for you. I will remind members they have 10 business days to submit questions for the records, and I ask the witnesses to respond to their questions promptly. Members should submit their questions by the close of business June 17.

Without objection, the subcommittee is adjourned.

[Whereupon, at 12:46 p.m., the subcommittee was adjourned.]