Feb 27 2019 11:30:13
TRANSCRIPT

February 26, 2019

COMMITTEE HEARING

REP. JAN SCHAKOWSKY, D-ILL.

WASHINGTON, DC

HOUSE ENERGY AND COMMERCE COMMITTEE, CONSUMER PROTECTION AND COMMERCE SUBCOMMITTEE HEARING ON **PROTECTING CONSUMER PRIVACY** IN THE

ERA OF BIG DATA

Bloomberg Government

Support: 1-877-498-3587

www.bgov.com

HOUSE ENERGY AND COMMERCE COMMITTEE, CONSUMER PROTECTION AND

COMMERCE SUBCOMMITTEE HEARING ON **PROTECTING CONSUMER PRIVACY** IN

THE ERA OF BIG DATA

FEBRUARY 26, 2019

SPEAKERS:

REP. JAN SCHAKOWSKY, D-ILL., CHAIR

REP. TONY CARDENAS, D-CALIF.

REP. BEN RAY LUJAN, D-N.M.

REP. DEBBIE DINGELL, D-MICH.

REP. DORIS MATSUI, D-CALIF.

REP. LISA BLUNT ROCHESTER, D-DEL.

REP. KATHY CASTOR, D-FLA.

REP. ROBIN KELLY, D-ILL.

REP. TOM O'HALLERAN, D-ARIZ.

REP. JERRY MCNERNEY, D-CALIF.

REP. BOBBY L. RUSH, D-ILL.

REP. DARREN SOTO, D-FLA.

REP. MARC VEASEY, D-TEXAS

REP. FRANK PALLONE JR., D-N.J., EX OFFICIO

REP. CATHY MCMORRIS RODGERS, R-WASH., RANKING MEMBER

REP. BOB LATTA, R-OHIO

REP. MICHAEL C. BURGESS, R-TEXAS

REP. BRETT GUTHRIE, R-KY.

REP. FRED UPTON, R-MICH.

REP. LARRY BUCSHON, R-IND.

REP. E.L. "BUDDY" CARTER, R-GA.

REP. GREG GIANFORTE, R-MONT.

REP. RICHARD HUDSON, R-N.C.

REP. GREG WALDEN, R-ORE., EX OFFICIO

WITNESSES:

BRANDI COLLINS, SENIOR CAMPAIGN DIRECTOR FOR MEDIA, DEMOCRACY &

ECONOMIC JUSTICE AT COLOR OF CHANGE

DAVE GRIMALDI, EXECUTIVE VICE PRESIDENT FOR PUBLIC POLICY AT

IAB

ROSLYN LAYTON, VISITING SCHOLAR AT THE AMERICAN ENTERPRISE

INSTITUTE

NUALA O'CONNOR, PRESIDENT AND CEO OF THE CENTER FOR DEMOCRACY &

TECHNOLOGY

AND DENISE ZHENG, VICE PRESIDENT FOR TECHNOLOGY, INNOVATION AT

THE BUSINESS ROUNDTABLE, TESTIFY

SCHAKOWSKY: Committee on Consumer Protection and Commerce will

now be called to order. So I'm going to begin with a few comments that are off the clock and then invite our ranking Member to do the same.

I want to say good morning and thank you all for joining us today. And before we officially start the hearing, I'd like to welcome you to the first Consumer Protection and Commerce Subcommittee of the 116th Congress.

Consumer protection has long been my passion and what first drew me to public life. I like to call our subcommittee the nation's legislative helpline, because we field consumer complaints. The subcommittee's jurisdiction is vast in scope, ranging from the safety of cars to consumer product defects to consumer fraud, both online and offline.

In the past when Democrats controlled the House, this subcommittee was responsible for making pools and children's products safer, increase the fuel efficiency of cars, and made sure agencies aggressively protect consumers over corporate interests. Under my leadership, this subcommittee will be extremely active and push companies and the administration to put consumers first.

I look forward to working with Ranking Member McMorris Rodgers. I believe there are so many issues on which we will be able to work together in a bipartisan way.

I'd also like to welcome several new Democratic members, Representative Marc Veasey from Texas. Let see. I'm looking the wrong way. Okay, from - and Robin Kelly from Illinois, my home state; Tom O'Halleran from Arizona; Lisa Blunt Rogers from Delaware; and Darren Soto from Florida are all new to the Energy and Commerce Committee and they also were smart enough to pick this best subcommittee at a - at a very exciting time.

I also welcome back many familiar faces and appreciate your continued commitment to consumer protection issues. And I would like to thank Tony Cardenas for serving as vice chair of the - of the subcommittee. And he will provide the subcommittee with invaluable leadership.

And, finally, I'd like to recognize the return of my friend, Debbie Dingell. Over the past two weeks, we have mourned the passing of her husband, John Dingell, who was so important to this committee over the years and a friend to so many.

Debbie has been a stalwart, but I know it has been a difficult time. Debbie, you have all of our sympathy and support from the entire subcommittee. And with the indulgence of my ranking member, just to say let Debbie say a few words. Debbie?

DINGELL: I just want to thank you all my colleagues. John

Dingell loved this committee. He thought the work that they did was very important. And I hear him in my ear going, "Woman, get on," and hearing him in the ears of everybody. Work together for the American people. Thank you.

SCHAKOWSKY: I've been reminded that Darren Soto's birthday is

today. Oh, yesterday? Okay. Never mind. Okay. So, Ranking Member McMorris Rodgers, would you like to take a couple of minutes to welcome your new members as well?

RODGERS: Thank you. Thank you, Madam Chair and to all the

members of the committee. Welcome to the committee. And I, too, want to extend my heartfelt thoughts and prayers to Debbie.

And I so appreciate her friendship, her leadership on this committee. And I would join in saying let's work together, as John Dingell would challenge us, "Let's work together for the American people." And it's great to have you back, Debbie.

To the new members of the committee, I'd like to recognize some of the newest members on our side of the aisle, Mr. Hudson from North Carolina - he'll be here shortly; Mr. Carter from Georgia; Mr. Gianforte from Montana. And I also have the privilege of having former chairman on this side of the aisle, Bob Latta and Burgess, and well as full committee chairman on this subcommittee.

I look forward to working with you, Madam Chair, on putting consumers first while ensuring that we continue to celebrate the innovation and all that it has meant to American, to the American way of life and improving our quality of life. As Americans, we've led the world in technology and innovation. And I look forward to the many issues that are before this committee and working to find that bipartisan ground wherever possible. Thank you, Madam Chairman.

SCHAKOWSKY: Let's take on that. All right. All right. So, I

yield myself five minutes now for an opening statement.

And as I said earlier, our subcommittee is the nation's legislative helpline. And our first hearing, "**Protecting Consumer Privacy** in the Era of Big Data," couldn't be more timely because the phone at the end of the helpline is ringing off the hook.

According to a recent survey, over 80 percent of U.S. adults were not very confident in the security of personal information held by social media, retail, and travel, and travel companies. And 67 percent wanted the government to act to protect them.

There is good reason for consumers' suspicion. Modern technology has made the collection, analysis, sharing, and the sale of data both easy and profitable. Personal information is mined from Americans with little regard for the consequences.

In the last week alone, we learned that Facebook exposed individual privacy, private health information. And they thought was - that consumers thought was protected in closed groups.

And collected - and Facebook also collected data from third-party app developers on issues as personal as women's menstrual cycles and cancer treatments. People seeking solace may instead find increased insurance rates as a result of the disclosure of that information.

But Facebook isn't alone. We have seen the data collection industry transfer - transform from a nascent industry most Americans haven't heard of to an economic powerhouse gobbling up every piece of consumer data it can, both online and offline.

While many companies claim to provide notice and choice to consumers, the truth is that providers - that they provide little reason for or believing we're protected.

Who has the time to wade through the dozens of privacy policies that impact them? How many people think about being tracked through their phones or by the overhead light in a - in a store? And often, only choice, the only choice they have to avoid data collection is not to go to the store or to use the app.

Reports of the abuse of personal information undoubtedly give Americans the creeps. But this data isn't being collected to give you the creeps. It's being done to control markets and make a profit. Without a comprehensive federal privacy law, the burden has fallen completely on consumers to protect themselves and this has to end.

Without a doubt, there are legitimate and beneficial reasons for consumers to use personal - for companies to use personal information, but data collection must come with responsibilities. There should be limits on the collection of consumers' data, and of the use and sharing of their personal information.

My goal is to develop strong, sensible legislation that provides meaningful protections for consumers while promoting competitive markets and restoring Americans' faith in business and government.

Rules alone, though, are not enough. We also need aggressive enforcement. Unfortunately, in recent years, the Federal Trade Commission's enforcement actions have done little to curb the worst behavior in data collection and data security.

Any legislation must give federal regulators the tools to take effective action to protect consumers. It is important to equip regulators and enforcers with the tools and funding necessary to protect privacy. But it is also critical to make sure that requests for more tools and privacy are not used as an excuse for inaction.

We must understand why the FTC hasn't used its existing suite of tools to the full extent, such as Section 5 authority to ban unfair methods of competition or its ability to enforce violators.

So I welcome our witnesses today to learn about how we should achieve these goals. Given the breadth of the issue, this will be the first of several hearings. Others will allow us to focus on specific issues of concern to the public.

So I look forward to working with all of you on both sides of the aisle. And I now yield to Ranking Member Cathy McMorris Rodgers for five minutes.

MCMORRIS RODGERS: Thank you, Madam Chair. I would like to thank you for organizing this first hearing of the Congress on privacy and security. It really builds on important work that was done in the past by Chairman Walden and Latta in the last Congress, and then Chairman Upton and Burgess in the 114th Congress.

I'm hopeful that we can find a bipartisan path to move forward on a single American approach to privacy, one that is going to protect consumers and individual privacy; one that ensures that consumers continue to benefit from the amazing technology and innovation that has happened in recent years.

This morning, I'd like to lay out four principles as we approach this effort, one that supports free markets, consumer choice, innovation and small businesses, the backbone of our economy. We often celebrate small businesses in America.

Principle number one, one national standard. The Constitution was crafted around the concept that one national marketplace would make America stronger in certain areas. It also recognizes the importance of intellectual property rights, free expression, and the rights of "We, the People" to be protected from the power of government.

The internet knows no borders. It's revolutionized our nation's economy by seamlessly connecting businesses and people across the country. Online, a small business in Spokane, Washington, can as easily reach customers in Illinois and New Jersey as in eastern Washington. Distance is no longer a barrier. The internet economy is interstate commerce and subject to federal jurisdiction.

There is a strong groundswell of support for a federal privacy law that sets a national standard. Many recognize the burdens multiple state laws would create.

But what would it mean for someone in Washington State who buys something online from a small business in Oregon to ship to their family in Idaho? This is a regulatory minefield that will force businesses to raise prices on their customers. Setting one national standard makes common sense, and it's the right approach to give people certainty.

Principle number two, transparency and accountability; companies must also be more transparent when explaining their practices. For example, we learned last week that Google included a microphone in their Nest device but failed to disclose it. And Facebook is collecting very personal health information from apps -- the chair mentioned that.

Transparency is critical. When unfair or deceptive practices are identified, there should be enforcement and there should be consequences strong enough to improve behavior.

Principle number three, improving data security. Another area important to this debate is data security. Perfect security doesn't exist online, and companies are bombarded by hackers every second of every day.

Certain data is more valuable on the black market, which is why Social Security numbers, credit card data, and login credentials are always major targets for criminals.

One goal must be to improve people's awareness for one, how their information is being collected and used; and two, how companies are protecting it, and how people can protect themselves.

Our focus should be on incentivizing innovation security solutions and certainty for companies who take reasonable steps to protect data. Otherwise, we risk prescriptive regulations that cannot be updated to keep up with the bad actors' newest tactics.

Principle number four, small businesses. We must not lose sight of small and medium-sized businesses and how heavy-handed laws and regulations can hurt them. Established bigger companies can navigate a complex and burdensome privacy regime. But millions of dollars in compliance costs aren't doable for startups and small businesses.

We have already seen this in Europe, where GDPR has actually increased, has helped increase the market share of the largest tech companies while forcing smaller companies offline with millions of dollars in compliance costs.

These startups and small businesses could be innovating the next major breakthrough in self-driving technology, health care, consumer - customer service, and so many other areas.

To keep America as the world's leading innovator, we cannot afford to hold them back. Heavy-handed and overly cautious regulations for all data will stop innovation that makes our roads safer, healthcare more accessible, and customer service experiences better.

I'm glad our teams were able to work together on today's hearing. This is a good step forward in finding a bipartisan solution for these critical issues.

And as we move forward, I'm sure there's going to be more hearings in the future to allow more small business owners, startups, and entrepreneurs to join the conversation. I believe we have a unique opportunity here for a bipartisan solution that clear - that sets clear rules for the road on data privacy.

In its best use, data has made it possible for grocery aisles to be organized on how people shop. But we can - we need to explore data privacy and security with forward-thinking solutions. And I look forward to hearing from the witnesses and being a part of this discussion today. Thank you very much, Madam Chair.

SCHAKOWSKY: Thank you. The gentlelady yields back. And now the

chair recognizes Mr. Pallone, chairman of the Full Committee for five minutes for his opening statement.

PALLONE: Thank you. I also wanted to welcome back Debbie

Dingell. Debbie's shown tremendous strength and courage during the past few weeks. And you were missed, Debbie. We're glad you're back today. So I just wanted to say that.

Welcome to the first hearing of the Consumer Protection and Commerce Subcommittee. We renamed the subcommittee to emphasize the importance of putting consumers first. And that is the lens through which I view the important issue of consumer privacy. How do we empower consumers and impose reasonable limits on companies that collect and use our personal information?

In the past, we've talked about major data breaches and scandals involving the misuse and unauthorized sharing of people's data. And we've talked about the potential for emerging technologies to be used in unintended and potentially harmful ways.

But privacy isn't just about major incidents or predictions of the future. It's an everyday issue, constantly affecting our lives and the lives of our children.

Almost every company that we interact with, and even many we don't, are conducting surveillance of us. When we visit a single website, many companies are tracking our actions on that site -- what we click on, how long we are on each page, even our mouse movements. And that's true for each of the dozens of sites most of us visit every day.

When we go out, our location is tracked on our phones. Video surveillance at stores, on the street, and in doctors' offices record what we do and who we are with. The purchases we make in stores are recorded by the stores through store loyalty programs, and by the credit cards we use to make those purchases.

And companies use that information to sort and commodify us, too. Inferences are drawn and we are labeled as a Democrat or Republican, white or Latino, gay or straight, a pregnant teen, a grieving parent, a cancer survivor, and so many more. This is all done without our knowledge.

And then our personal information and related inferences are being shared and sold many times over. Companies may share our information with business partners and affiliates that we have never heard of.

Our data also may be sold to data brokers, who collect massive amounts of data about all of us, and then sell that off to anyone willing to pay for it. The scope of it all is mindboggling.

Without a doubt, there are positive uses of data. Companies need personal information to deliver a package or charge for a service. Some data is used for research and development of new products and improving services. And sometimes it's used for fraud prevention or cybersecurity purposes. And some of it is used for scientific research to find new treatments for medical conditions.

But in some cases, data use results in discrimination, differential pricing, and even physical harm. Low-income consumers may get charged more for products online because they live far away from competitive retailers.

Health insurance companies could charge higher rates based on your food purchases or info from your fitness trackers. A victim of domestic violence may even have real-time location tracking information sold to their attacker.

And these are simply unacceptable uses of people's data. Yet, for the most part, here in the U.S., no rules apply to how companies collect and use our information. Many companies draft privacy policies that provide few protections and are often unread.

One study calculated that it would take 76 years to read all of the privacy policies for every website the average consumer visits each year. And even if you could read and understand these privacy policies, often your only choice is to accept the terms or not use the service.

In a lot of situations, that is simply not an option. Consider when you need to pay for parking at a meter or use a website for work, you don't really have that choice. So we can no longer rely on a "notice and consent" system built on such unrealistic and unfair foundations.

As the chairwoman said, we need to look toward to its comprehensive privacy legislation, legislation that shifts the burden off consumers and puts reasonable responsibility on those profiting from the collection and use of our data.

Because consumer privacy isn't new to this committee. We've been talking about it for years, yet nothing has been done to address the problem. And this hearing is the beginning of a long overdue conversation. It is time that we move past the old model that protects the companies using the data, and not the people.

So I look forward to hearing from our witnesses today on how we can work together to accomplish this. I plan to work with my colleagues on both sides of the aisle to craft strong, comprehensive privacy legislation that puts consumers first.

And I just want to thank you, Chairman Schakowsky when you said that what this committee is all about is putting consumers first. And I think that having this hearing as you are today on the privacy issue is a strong indication that that's exactly what we intend to do. Thank you again.

SCHAKOWSKY: I thank the gentleman. The gentleman yields back.

And now the Chair recognizes Mr. Walden, ranking member of the Full Committee for five minutes for his opening statement.

WALDEN: Well, good morning, and welcome to our members and

witnesses. Congratulations to both Representative Rodgers as the new lead Republican and to Representative Jan Schakowsky as the new chair for the Consumer Protection and Commerce Subcommittee. I know we're off to a good start this morning.

We have a lot of important issues to work on in this subcommittee, and I am hopeful we can continue the bipartisan achievements out of this subcommittee. From Chair Schakowsky and Representative Latta's SELF DRIVE Act, to legislation focused on the internet of Things, and oversight of the FTC, CPSC. and NHTSA. I hope we can continue working together for the benefit of the American consumer.

I would like to thank Chairs Pallone and Schakowsky for picking up the privacy and security issues as the topic of the first hearing for the subcommittee. From the Disrupter Series of hearings that we held in last Congress, to the first congressional hearings with major tech company CEOs, this committee has been on the forefront of getting answers for our constituents.

The debate over privacy? It's not new. From the first Kodak camera to caller-ID, major privacy debates ensued when the new innovation was introduced.

But there are new challenges when it comes to privacy, and we've heard some of that today from our members. Privacy means different things to different people, which makes this debate even more challenging in the age of Instagram and YouTube.

I believe it's important that we work together toward a bipartisan federal privacy bill that, one, improves transparency, accountability, and security for consumers. That, two, protects innovation and small businesses. And three, sets one national standard.

Now, the first issue that some like to frame as incredibly divisive, falls under the most basic principle underpinning our jurisdiction. And that is the term "interstate commerce."

A federal privacy bill needs to be just that, one that sets the national standard for commercial collection, use, and sharing of personal data in the best interest of consumers.

The Supreme Court has recently reaffirmed the principles of the Commerce Clause. State laws cannot discriminate against interstate commerce. They cannot impose undue burdens on interstate commerce, and should take into consideration the small businesses, startups, and others who engage in commerce across state lines.

There are many policy areas where it makes sense for states to innovate; however, the internet does not stop at the state line and neither should innovation - and innovative privacy and security solutions.

Your privacy and security should not change depending on where you are in the United States. One state should not set the standards for the rest of the country.

We can improve the security and privacy of consumers' data without adding to the confusion or harming small businesses and entrepreneurs. So Congress should thoughtfully consider what various states are proposing so we can deliver that certainty and do so with a national standard.

We can learn from California and we can learn from Washington, and a growing number of other states who have drafted their own legislation, reinforcing why we should begin with an agreement that a federal privacy bill sets one national standard.

Now, a truly American approach to privacy and security can give consumers better control by supporting innovative solutions without massively expanding the regulatory state. We should avoid creating a system that floods people's inboxes with privacy policies that, frankly, they do not read, or click-through notices that make even simple tasks very frustrating.

We can and should, however, learn from previous efforts here at home and abroad. So, transparency and accountability are critical to move forward and measurably improve consumers' ability to choose between services they want to use. People need to receive a clearer understanding of exactly how their data are used by the digital services with whom they interact.

The FTC has announced their investigation into both Equifax and Facebook. The outcome of their work will help Congress evaluate the effectiveness of laws currently on the books and the enforcement tools utilized to hold companies accountable.

We can write bill after bill, and the FTC could publish rule after rule. But if we do not have effective enforcement, they are just words on paper. So I believe we have a unique opportunity to address some of the most complex privacy and security questions of the day.

And I look forward to working with my colleagues across the aisle on setting a national framework and getting this debate moving forward towards a bipartisan national solution. With that, Madam Chair, I yield back.

SCHAKOWSKY: Thank you. The gentleman yields back. And the chair

would like to remind members that pursuant to committee rules, all members' written opening statements shall be made part of the record.

And now, I would like to introduce our witnesses for today's hearing and thank you all for coming. We have Ms. Brandi Collins-Dexter, senior campaign director, media, democracy and economic justice at Color of Change.

Dr. Roslyn Layton, visiting scholar at the American Enterprise Institute. Ms. Denise Zheng - is that correct, Zheng? Okay - vice president, technology, innovation, Business Roundtable.

Dr. Dave Grimaldi, executive vice president for public policy, IAB. And Dr. Nuala O'Connor, President and CEO of the Center for Democracy & Technology. And let's begin then with Ms. Collins-Dexter.

COLLINS-DEXTER: Good morning, Madam Chair, Ranking Member

Rodgers, Committee Chairman Pallone, Committee Ranking Member Walden, and members of the subcommittee.

My name is Brandi Collins-Dexter, and I am a senior campaign director at Color of Change, the largest online civil rights organization in the United States, with more than 1.5 million members who use technology to fight for change.

In the Wild, Wild West of the digital economy, discriminatory marketing practices are so lucrative that entire industries have sprung up to discriminate for dollars.

One company called "Ethnic Technologies," subtle I know, developed software that predicts an individual's ethnic origin based on data points easily purchased from ISPs and then sells that data which has been turned into a predictive algorithm to any company that wants to target groups or services to a particular ethnic group.

Part of what we're seeing now is bad online behavior that circumvents civil rights laws. Google and Facebook have both had numerous complaints filed against them for allowing discriminatory housing and employment acts.

State commission reports found that voter suppression ads were explicitly targeted towards black Americans on social media during the 2016 presidential election. And that social media companies may misleading or evasive claims about those efforts.

Additionally, low-income communities are targeted by predatory payday loan companies that make billions of dollars in interest and fees on the back of struggling families. We've seen the online price gouging and digital redlining where corporations like Staples have used geotracking and personal data to charge customers higher prices for products based on their geography.

Some data brokers even lump consumers into categories like, quote, unquote, "Getting by", "compulsive online gamblers." One company has even used a category called "Speedy Dinero" described as, quote, "Hispanic communities in need of fast cash receptive to subprime credit offers."

Last week, as was mentioned, Facebook was caught obtaining sensitive personal information submitted to entirely separate mobile apps, using software that immediately shares data with social networks for ad targeting. I mean, literally my iPad knows more about me than my husband, and he is an ex-journalist who is very nosy.

Even information that feels innocuous can become a proxy for a protected class and sensitive information. Right now, corporations are able to easily combine information about you they purchased and create a profile of your vulnerabilities.

Earlier this month, Color of Change joined with advocacy groups to urge Congress to put civil and human rights at the center of the privacy fight.

Our letters states in part, "Civil rights protections have existed in brick-and-mortar commerce for decades. Platforms and other online services should not be permitted to use consumer data to discriminate against protected classes or deny them opportunities in commerce, housing, and employment, or full participation in our democracy."

There are many bills out there, some we think are weak and some like language we've seen from Senator Cortez Masto, show a great deal of promise.

But, ultimately, we would like to see bipartisan legislation written through an anti-discrimination lens that prevents manipulative or exclusionary marketing practices that exacerbate poverty. It should offer a baseline that does not preempt innovative state policy. And it must contain enforcement mechanisms and not rely on self-regulation.

Some say privacy is the currency you pay to engage in our digital ecosystem. We should not have to make that choice. Our communities need to trust that when we go online we can count on our privacy and the safety of our information for ourselves and our children.

This shouldn't be a game of political football, 80 percent of Americans support making it illegal for companies to sell or share their personal information. At least 80 percent of us believe that we should have control over how companies use our personal information.

Privacy is a concept in its most aspirational sense. It's not merely about the freedom and ability to close your digital curtains, so to speak. Instead, we should consider privacy and digital rights for all a necessary framework crucial for ensuring that our human, civil, and constitutional rights are not confined to our offline lives but are also protective online where so much of our daily life occurs.

I would even say that if we fail in the mission to ensure our rights online are protected, we stand to render many of our offline rights meaningless. Thank you again for having me here today and I look forward to your thoughts.

SCHAKOWSKY: Thank you. I meant to mention that each of you has

five minutes. And I appreciate you, Ms. Collins-Dexter for sticking to that. The lights that will go on initially will be green. And then the light will turn yellow when you have one minute remaining. And then red means you need to stop.

And so, Dr. Layton, you are recognized for five minutes.

LAYTON: Good morning. Thank you, Chair Schakowsky, Ms. McMorris

Rodgers and members of the committee. It's an honor to be here, and I am heartened by your bipartisanship.

Today, I represent only myself and my research. I've lived in the European Union for the last decade and I work at a European University where I make international internet policy comparisons. As the mother of three Danish-American children, I'm legitimately interest in policy that makes Europe a better place.

The academic literature shows that online trust is a function of institutions, business practices, technologies, and users' knowledge. But, unfortunately, the EU rejected this formula for its data protection policy.

My hope is that Congress will avoid the mistakes of the GDPR and ultimately leapfrog Europe with a better framework based upon privacy enhancing technologies, a strong federal standard, and consumer education.

To analyze a policy like the GDPR, we must evaluate its real-world effects. Since its implementation, Google, Facebook and Amazon have increased their market share in the EU. This is a perverse outcome for a policy promised to level the playing field.

Today, only 20 percent of EU companies are online. There's little to no data that shows that small and medium-sized enterprises are gaining as a result of the GDPR. The data shows that consistent lag in the small to medium-sized business segment, particularly for them to modernize their websites and market outside their own EU country.

Now, this income - this outcome isn't necessarily surprising. As the Nobel Prize Economist George Stigler observed 40 years ago, "Regulation is acquired by industry and operated for its benefit."

A number of large companies have come out in support of the GDPR. It doesn't surprise me either, that's because it cements their market position. They don't need permissionless innovation anymore but they don't have a problem depriving startups with the same freedom.

Now, to comply with the GDPR today, an average firm of 500 employees will spend about $3 million and thousands of U.S. firms have decided that this is not worthwhile, including the Chicago Tribune which is no longer visible in the European Union.

There are over 1,000 American news media that no longer reach Europeans. This is also concerning because the EU is a destination of two-thirds of America's goods and services.

Now, the GDPR might be justified if it creates a greater trust in the digital ecosystem but there is no such evidence. After a decade of these kinds of data protection regulations in which users endure intrusive pop-ups and disclosures in every digital site they visit, Europeans report no greater sense of trust online.

More than half of the survey respondents in the U.K. alone say that they feel no better since the GDPR took effect. And it has not helped them to understand how their data is used.

I'm skeptical of both the GDPR and the CCPA in California with their laundry list of requirements, 45 in Europe and 77 in California. These are not scientifically tested and there is no rational policy process to vet their efficacy.

Now, I imagine if we held - now what happen if we would hold government to the same standards? Australia tried a "when in doubt, opt out policy" and half a million people left the National Healthcare Record Program. It crashed their system for healthcare.

We have another reason to be skeptical of the claims of the EU being morally superior with their GDPR. Their networks are not secure because they're built with equipment by dubious Chinese equipment makers. Your data protection standard means little if the Chinese government can hack your data through backdoors.

In any event, Europe's attempt to create a common market for data is something that was actually part of our founding in, of our country with our national standard interstate commerce which has been discussed. And I support such a national standard for sensitive data consistently applied across enterprises.

To leap the Europeans on data protection, we need to review the empirical research that the Europeans ignored, namely, how privacy enhancement technologies and user knowledge will promote online trust.

The answer is not to copy the EU but to build world class, scientifically superior privacy enhancing technology here in the United States. Congress should incentivize the development of such technologies through grants and competitions, and provide safe harbors for their research, development and practice.

There is no consumer protection without consumer education. And we should support people to acquire their digital competence so they can make informed decisions about the products they use.

In closing, please do not fall prey to the European regulatory fallacy which substitutes the bureaucratization of data instead of a natural right of privacy.

Increasing the number of agencies and bureaucrats who govern our data does not increase our privacy. It reduces our freedom, makes enterprise more expensive, and deters innovation. Thank you for your leadership. I welcome your questions.

SCHAKOWSKY: Thank you. Ms. Zheng, you are recognized for five

minutes.

ZHENG: Thank you, Chairwoman Schakowsky, Ranking Member

McMorris Rogers.

SCHAKOWSKY: Microphone. There you go.

ZHENG: I'm sorry. Chairwoman Schakowsky, Ranking Member

McMorris Rogers, members of the subcommittee, thank you for the opportunity to testify on behalf of the Business Roundtable.

Business Roundtable represents more than 200 CEOs of the largest American companies that operate in nearly every corner of the economy, including technology, telecommunications, retail, banking, health, manufacturing, automotive, and many other industries.

Our companies touch virtually every American consumer. They processed 16 trillion in global consumer payments each other and service roughly 40 million utilities customers across the

country.

They fly more than 250 million passengers to their destination each year and provide wireless communications and internet services to more than 160 million consumers. Respond to nearly 70 million medical insurance memberships and deliver more than 42 million packages every single day.

Data privacy is a major priority for the Business Roundtable, especially of companies that rely on data and digital platforms to deliver products and services to consumers and to conduct day to day business operations.

That is why CEOs from across industry sectors have come together to call for a federal privacy law that provides consistent consumer privacy protections, promotes accountability, and fosters innovation and competitiveness.

We strongly support giving consumers control over how their personally identifiable information is collected, use and shared. At the same time, it is important to remember the value of data in our economy, as well as the enormous benefits that data-driven services provide to our consumers.

Data enable companies to deliver more relevant and valuable user experiences to consumers. It allows the companies to detect and prevent fraud on user accounts and combat cybersecurity attacks.

It creates greater productivity and cost-savings from manufacturing to transportation and logistics. And it leads to breakthroughs in health and medical research. Innovation thrives in stable policy environments, where new ideas can be explored and flourish within a well-understood legal and regulatory framework.

So, in December, Business Roundtable released a proposal for privacy legislation. Our proposal is the product of extensive deliberation with the chief privacy officers of our companies and approval from CEOs across industry sectors.

We believe that privacy legislation must prioritize four important objectives. First and foremost, it should champion consumer privacy and promote accountability. Legislation should include strong protections for personal data that enhance consumer trust and demonstrate U.S. leadership as a champion for privacy.

Second, is fostering innovation and competitiveness, especially in a dynamic and evolving technology landscape. Legislation should be technology neutral and allow organizations to adopt privacy protections that are appropriate to specific risks, such as the sensitivity of the data.

Third, it should harmonize privacy protections. Congress should enact a comprehensive national law that ensures consistent protections and avoid the state by state approach that leads to disjointed consumer protections, degraded user experience, and barriers to investment and innovation.

And fourth, legislation should promote consumer privacy regimes that are interoperable on a global basis. And it should the bridge differences between the U.S. and foreign privacy regimes.

At the heart of the Business Roundtable proposal is our set of core individual rights that we believe consumers should have over their data including transparency.

Consumers deserve to have clear and concise understanding of the personal data that a company collects, the purposes for which that data is used, and whether and for what purposes personal data is disclosed to third parties.

Control. Consumers should have meaningful control over their data based upon the sensitivity of the information, including the ability to control whether that data is sold to third parties.

Consumer should also have the right to access and correct inaccuracies in their personal data about them; and they should have the right to delete personal data.

A federal privacy law should be comprehensive and apply a consistent, uniform framework to the collection, use and sharing of data across industry sectors.

It should also recognize that there are situations that do justify exceptions, such as cases of public health and safety, or to prevent fraud and provide cybersecurity, or when certain data is necessary to deliver a product or a service that the consumer requested, or to ensure First Amendment rights and to protect the rights of other individuals.

Establishing and protecting these consumer rights also requires effective, consistent and coordinated enforcement to provide accountability and protect consumer rights.

Absent action from Congress, we will be subject not only to a growing, confusing set of state government requirements but also to different data protection laws from governments in Europe, countries like Brazil and elsewhere.

Make no mistake; consumers deserve meaningful, understandable and consistent privacy rights regardless of where they live or where their data may be located.

I thank the subcommittee for its leadership in holding this hearing and for encouraging a dialogue. And I look forward to the questions. Thank you.

SCHAKOWSKY: Thank you. Mr. Grimaldi, you are now recognized for

five minutes.

GRIMALDI: Thank you, Chairwoman Schakowsky, Ranking Member

Rodgers, and members of the committee. I appreciate the opportunity to testify here today.

I am Dave Grimaldi, Executive Vice President for Public Policy at the Interactive Advertising Bureau which was founded in 1996. Headquartered in New York City, we represents over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns.

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate.

Data-driven advertising also allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a 2017 study, in 2016 the U.S. ad-supported internet created 10.4 million jobs and added $1.1 trillion to the U.S. economy. The study designed to provide a comprehensive review of the entire internet economy and answer questions about its size, what comprises it and the economic and social benefits Americans drive from it revealed key findings that analyze the economic importance as well as the social benefits of the internet.

And indeed as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that could become available in the future.

The time is right for the creation of a new paradigm for data privacy in the United States. And IAB working with Congress and based on our members' successful experience creating privacy programs that consumers understand and use, can achieve a new federal approach that, instead of bombarding consumers with notices and choices, comprehensively describes clear, workable, and consistent standards that consumers, businesses, and law enforcers can rely upon.

Without a consistent federal privacy standard, a patchwork of state privacy laws will create consumer confusion, present substantial challenges for businesses trying to comply with these laws, and fail to meet consumers' expectations about their digital privacy. We ask Congress to standardize privacy protections across the country by passing legislation that provides important protections for consumers while allowing digital innovation to continue to flourish.

We caution Congress not to rely on the frameworks set forth in Europe's General Data Privacy Regulation or California's Consumer Privacy Act as examples of the ways in which a national privacy standard should function.

Far from being a desirable model, the GDPR shows how overly restrictive frameworks can be harmful to competition and consumers alike. Less than a year into GDPR's applicability, the negative effects of its approach have already become clear. The GDPR has led directly to consumers losing access to online resources, with more than 1,000 U.S.-based publishers blocking European consumers from access to online material in part because of the inability to profitably run advertising.

To that unfortunate end, as was pointed out before, I would note that the Chicago Tribune including its Pulitzer Prize-winning stories on government corruption, faulty government regulation, et cetera, is no longer accessible in Europe due to GDPR.

Additionally, the San Fernando Sun newspaper which has been open since 1904 is no longer accessible and the Holland Sentinel founded in 1896 can no longer be seen in Europe.

Small businesses and startups also saw the negative impact of the GDPR, with many choosing to exit the market. Consent banners and pop-up notices have been notably ineffective at curbing irresponsible data practices or truly furthering consumer awareness and choice. The CCPA follows in the footsteps of GDPR and could harm consumers by impeding their access to expected tools, content, and services, and revealing their personal information to unintended recipients due to the lack of clarity in the law.

To achieve these goals, IAB asks Congress to support a new paradigm that would follow certain basic principles. First, in contrast to many existing privacy regimes, a new law should impose clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified in the law. Consumers will then be protected from such practices without the need for any action on their part.

Second, a new law should distinguish between data practices that pose a threat to consumers and those that do not, rather than taking a broad-brush approach to all data collection and use. And

finally, the law should incentivize strong and enforceable compliance and self-regulatory programs, and thus increase compliance by creating a rigorous safe harbor process.

IAB asks for Congress's support in developing such a framework. We look forward to partnering with you to enhance consumer privacy. Thank you for your time today and I welcome your questions.

SCHAKOWSKY: Thank you. Ms. O'Connor you're recognized for five

minutes.

NUALA O'CONNOR: Chairman Schakowsky, Ranking Member McMorris Rodgers, members of the subcommittee, thank you for the opportunity to testify today.

My colleagues and I at the Center for Democracy & Technology are tremendously excited about the prospect of federal privacy legislation. We appreciate your leadership in taking on this challenging issue.

Privacy and data over the last several decades have become full of jargon and overly complexified. So I have one basic message today and that is notice and choice are no longer a choice. Any privacy legislation that merely cements the current status quo of the notice and consent model for personal data is a missed opportunity.

Let me take a moment to demonstrate why that status quo is not working for individual consumers and companies. If I could respectfully request the members and their staff to take out their phones, some of you already have them out, I hear them ringing, and take a look at the home page. Open it up with whatever you use to open up your phone, mine is my fingerprint and it's not working.

Now look at your homepage, how many apps do you have? I have 262 apps on my phone. I had 261 until Saturday night when the kids said, "Mom, we want Chipotle for dinner" and I had to download again the Postmates app, so now it's 262.

The average person has around 80 according to current research. You can call me an overachiever or just a working mom. But for each of these 80 or so applications, you have already given the company behind it your consent to use your personal data and likely in a variety of ways.

For some of those apps you're sharing your location data, others your financial data, your credit card numbers, some of your apps have information about your physical activity, your health and other intimate information even in real time.

Regardless of the types of data, you have received 80 notices and 80 different consents have already been given. Do you remember the personal data you agreed to consent to give? And do you remember the purposes for which you shared it? Do you have a good understanding of how the companies behind those apps and devices are going to use that information six weeks from now, six months, or six years from now?

Now let's assume for the sake of this demonstration that each of those 80 companies has even just a modest number of information sharing agreements with third parties. Back in 2015 which is the ancient times of the internet, the average smartphone app was already automatically sharing data with at least three companies and three different parties.

You don't know those companies, you don't have a direct relationship with them, and now they have your personal information because you were given notice and you consented, and that means the average smartphone user has given consent for their data to be used by at least 240 different entities.

That doesn't reflect how information is already being shared by the companies with vendors, corporate affiliates, business partners. In reality, the number is likely much higher. And that's just what's on your phone.

That 240 number doesn't account for your other devices, the devices in your daily life, in your house, in your car, your other online accounts, data initially collected in the non-digital world, loyalty programs, cameras, paper surveys, and public records.

Does that feel like you have control over your personal information? But you gave your consent at some point. Clearly, it's time for a change. Some will say that the way to fix this problem is just make more privacy policies, more notices, make them clearer so consumers can better understand those decisions.

More check boxes will provide the appearance of choice, but not real options for consumers. Pursuing legislation like this just doubles down on our current system of notice and choice and further burdens already busy consumers. There is fundamentally no meaningful way for people to make informed, timely decisions about the many different data collectors and processors with whom we interact every day.

Instead, the goal should be to define our digital civil rights. What reasonable behavior can we expect from companies that hold our data? What rights do we have that are so precious they cannot signed away?

The Center for Democracy & Technology has drafted comprehensive legislation that is already available and has been shared with your staff. I am happy to answer questions about it today. But

most importantly, our bill and any meaningful privacy legislation must first prohibit unfair data practices, particularly the repurchasing or secondary use of sensitive data with carefully scoped exceptions.

Two, prevent data-driven discrimination and civil rights abuses. Three, provide robust and rigorous enforcement. Reasonable data security practices and individual control of rights such as the right to access, correct, and delete your data are obviously essential. Enacting clear comprehensive rules will facilitate trust and cement America's economic and ethical leadership on technology.

Now is the time for real change. You have the opportunity to shape a new paradigm for data use and you have the support of the majority of Americans to do so. Thank you.

SCHAKOWSKY: Thank you. So we've now concluded our opening

statements and we now will move to member questions. Each member will have five minutes to ask questions of our witnesses and I will start by recognizing myself for five minutes.

So, this is a stack of really just some of the privacy policies of the websites, apps, stores, and other services I interacted with just yesterday and actually not all of yesterday. I haven't read them all. And I checked the weather on my phone, so I have a privacy policy for that app.

I flew into town yesterday, I have the privacy policy for the airline and for the online travel. In order to get onto the plane, I had to go to my phone. I used the app to book the flight, I went to the drugstore and used my loyalty card, so I have that privacy policy. I checked the news online, so I have a few privacy policies for a few of the newspaper sites that I visited. I watched TV, I went online, I used my cellphone, I have a privacy policy for my cable provider, my internet service provider, my cellphone, my cellphone manufacturer, and the operating system and that's still just some of them.

And at that point, did I have the option to proceed, and I didn't have the option at any point to proceed without agreeing to the terms. And frankly, I think like most consumers because I'm anxious to actually get the job done, I agree. I agree.

So this stack does not include each of their service providers or affiliates or the data broker that gets my information from them or a third party advertiser, advertising company, or analytic company, or whoever else is lurking unseen to me and unheard and unknown.

By the way, a lot of these policies are pretty vague about what they do with my data and who they share it with or sell it to. This is the limitation of the notice and consent system that we use right now. A person should not need to have an advanced law degree to avoid being taken advantage of. We need to find solutions that take the burden off the consumer and put some responsibilities on those who want our data.

So Ms. Collins-Dexter, can you talk a little bit about some of the ways that our data is being used by consumers, and then Ms. O'Connor if you could follow up.

COLLINS: Some of the ways in which your data is being used by

consumers?

SCHAKOWSKY: We're talking about being, I'm sorry. How it's

being used by companies no, I'm sorry.

COLLINS: Yes. It's being used in all sorts of (inaudible) ways

and I think to your point earlier, I think even if we know that our data is being used in a number of ways, I think a report was released last week that said black people are actually more likely to read the fine print before they sign on to things on the internet and have long believed that their information and data was being sold, and yet that hasn't made us particularly safer.

We still had to experience all sorts of ways in which our data is being used against us. Even data points that feels innocuous can be used as sort of proxies for protected class. I offered some examples in the document that I shared with you.

But another example comes from the insurance industry in the realm of car insurance for example. Auto insurance telematics devices will be considered "non-sensitive" data such as vehicle speed, the time of day someone is driving, the miles driven, the rates of acceleration and braking. Those devices aren't collecting what we would consider sensitive data such as location and driver's identity, and yet that information is being used to like charge people higher rates for insurance. And it happens that the people most likely to be driving at night, most likely to be braking, all of these things are usually like working lower class people.

SCHAKOWSKY: If I could interrupt and we'll get more of that but

I want to see if Nuala O'Connor want to say at least one thing to this.

O'CONNOR: Thank you so much. There's a primary purpose for

data. When you give your data to a company to deliver that yellow sweater, they need to know your name and address, that makes sense.

There are secondary purposes in terms of business processing and activities that might be legitimate where we feel in our drafts of legislation, secondary purpose for sensitive data like for example the fingerprint I was using to open my phone, I want to be able to open my phone with that, I don't want that sensitive biometric data used for a secondary purpose by that company or by other companies.

So we would say there's a higher level of sensitivity around biometric data, intimate or immutable information about you deserves second or higher level of care and also they're sharing. Obviously there's your data going from a first party to an entirely separate third party in transaction, that would lead concern and those parties should be bound by the promises that first party made.

SCHAKOWSKY: Thank you. And now let me recognize our ranking

member, Cathy McMorris Rodgers.

CATHY MCMORRIS RODGERS: Thank you Madam Chair. I appreciate again everyone being here and I do believe that there's bipartisan support to move forward so that we can ensure strong protection of personal data that will ensure that we are improving upon consumer trust and demonstrating U.S. leadership in privacy and innovation.

I am concerned about the past work of privacy and security laws that I see coming at the state level and we're moving forward in Washington State, there's a debate going on as well as other states that are taking action that I believe are going to lead to higher cost and impact on consumers, it's going to actually increase their prices and reduce the options that consumers have.

I'd like to start with Dr. Layton and just ask the question, do you think that is important for one federal privacy law to set that national standard and if so, just explain some more why.

LAYTON: Thank you for the question. I was heartened to hear our

panelists and our representatives agree that we do need a comprehensive federal standard. Because California is such a large economy, it can go forward with its particular rules, it can dictate the rules for the rest of America.

We've talked a lot about rights here on this panel and all Americans have rights and it isn't fair that one state gets to dictate for everyone else. We should certainly look at California and learn from them, but it is as I understand a law that came together and that was their choice about how they did it. So I certainly agree that we need a national standard.

MCMORRIS RODGERS: I would like to ask Mr. Grimaldi and Ms. Zheng if you also would address this question. And if your members agree with the one national standard.

GRIMALDI: Thank you congresswoman. We do. But make no mistake,

we are very much in favor of the concepts of transparency and accountability and choice which are the bedrocks of CCPA and the reason that Californians came together to rally behind a law and the merits in it.

But to echo what Dr. Layton said, that patchwork could have incredibly negative effects on the American interne economy because it will force compliance costs not just on California companies but on all companies in America. It will imbalance what the larger providers can pay for those compliance costs and to retrofit their systems and to get ready to field what will be likely a barrage of lawsuits and quite honestly just fewer users, meaning fewer advertising costs once the enforcement of CCPA goes into effect in January.

And that's not indicative of a good privacy policy that provides to consumers what they currently enjoy, their content, their news, their video, everything else.

ZHENG: I also completely agree. Thank you for that question

Ranking Member McMorris Rodgers. I think from the Business Roundtable perspective a national consumer privacy law should not mean that consumers get less protections than currently exist.

But we set the standard at appropriate level, it can mean that every American across this country has protections that they don't currently have. So when we developed our proposal we looked at the California Law, we looked at GDPR, we looked at other state proposals and FTC authority and tried to take the best practices of each of these individual laws in developing our proposal.

MCMORRIS-RODGERS: Great, and just as a follow-up, I think as we

move forward, we need to be very concerned about making sure that we're protecting individuals' privacy, but also ensuring that we're not becoming too regulatory, that where -- that the regulations are not too complex and -- and through that -- through the regulations actually helping, the largest

actors can pay those costs, but it will make it harder for our startups and our innovators to get -- to get in some marketplace.

Dr. Layton, would you just address what you've seen which GDPR to date, as far as the impact on businesses?

LAYTON: Yes. Well, in the case of the European Union, you have

a data protection authority in each state and you have a super regulator overseeing that. And when this has come into play, there was no training, there was no funding to help the particular agencies get up to speed. They're not all equipped with the same set of skills. Some -- some regulators may have worked there their whole life, other ones may be new, they have different set of expertise.

So -- and each country had its own particular rules. And this -- this issue in question around how do they manage this going forward, that even the framers of the GDPR themselves said it will be two years before we have a judgment because of the actual process and how long it takes and so on. So in the minds of the -- and the Europeans -- this was also an important, what they see as a way to empower government that they're looking to place people in jobs. They expect that they'd have 75,000 more bureaucrats working in these particular jobs to look over the privacy and so on.

So it's -- it's their sort of -- it reflects what's going on in the EU today is a desperation, there are many people dissatisfied with the European Union. You probably know about Brexit, and this is a way that the EU is trying to respond to demonstrate to constituents that they -- that the EU can do something. And it's not, you know, in the U.S., we might say, "Well, let's make it better and innovate."

MCMORRIS-RODGERS: If you could -- if you could wrap up.

LAYTON: Yeah, so that was my point. Thank you.

MCMORRIS-RODGERS: Thank you. I yield back.

SCHAKOWSKY: The time has expired, now the gentlelady from

Florida, Cathy Castor.

CASTOR: Thank you. You know, Americans are increasingly fed up

with the violation of their privacy by online companies. There is simply a massive amount of data being collected on each and every person and then when that data is used or misused without their permission of there's a breach of their financial data or their health data, I mean that is -- it's really outrageous we've let it get this far and I think American consumers understand that this -- this needs to be fixed.

So I want to thank Chairwoman Schakowsky for calling this hearing and I look forward to working with her and the other members on this committee to adopt strong privacy protections for American families and consumers.

Ms. O'Connor, help us asses the current state of Americans' online privacy protections. I'll -- let me know if you agree or disagree with these statements. Currently there is no general federal law that requires online companies to have privacy policies or protect our privacy, is that correct or not correct?

O'CONNOR: That is correct.

CASTOR: And there is no general federal law that requires an

online company to secure our personal information or notify a customer if his or her personal information has been stolen. Is that correct?

O'CONNOR: That is correct.

CASTOR: And the only way the Federal Trade Commission is able

to examine companies that violate our privacy is through Section 5, Unfair or Deceptive Acts or Practices Authority which basically means that companies can do whatever they want with our data as long as they don't lie about what they're doing. Is that right?

O'CONNOR: That is correct.

CASTOR: So it is accurate to say that a bad online actor can

collect all sorts of very personal information such as your location, your birthday, your messages, your biometric data, your Social Security number, political leanings without your permission and sell it to the highest bidder as long as they don't lie about what they're doing?

O'CONNOR: It's pretty -- pretty accurate.

CASTOR: Well that's -- that's outrageous, and I think that's

why American consumers now have -- there's been an awakening to -- to what has been happening. They understand this now and they're demanding strong privacy protections.

So one of the areas that concerns me the most, Ms. Collins, is the data that's collected on children. There is a bedrock federal law, the Children's Online Privacy Protection Act is supposed to protect kids from -- from data being gathered on them and being targeted, but it was signed into law over 20 years ago. And think about how much the internet has changed in 20 years, the -- the apps that are available to kids, the toys that talk to them and gather data. Do you agree that COPPA needs to be updated as well?

COLLINS-DEXTER: Yes, I do. Can I expand on that a little more?

CASTOR: Please. I noticed in your testimony, you cited the

Cal-Berkeley study where they've identified how many apps targeted to kids that -- that are probably gathering their data. Could you go into that very briefly?

COLLINS-DEXTER: Yes, yes. So, I mean I think in general COPPA

is the only federal internet privacy law in the books and beyond that I think it's a solid blueprint for what comprehensive privacy legislation could look like with an opt-in model and placing obligations on our companies for adequate disclosure.

But as you point out, it's 20 years old and like the Civil Rights Act, it does not account for the digital economy we're immersed in today. So as I mentioned, a Cal-Berkeley study found that thousands upon thousands of children's apps currently available on Google Play violate COPPA. The fact that the market is flooded with data collection apps and devices targeted at kids like Echo Dot, Cloudpad or Be Connect and others should alarm us.

More than one-third of U.S. homes have a smart toy and so it's really important for us to like really, you know, think of the implications of that as we look to modernize our legislation.

CASTOR: Because we -- we kind of have an understanding now that

online companies are building profiles on -- on all of us, with huge amounts of data. But they're doing this to our kids now notwithstanding the fact that we have a federal law that supposedly says you can't do this, is that right?

COLLINS-DEXTER: That is correct.

CASTOR: Ms. O'Connor, I don't think the average American parent

understands that the apps and the toys that are provided for their kids to have fun and play games are creating these shadow profiles. Is that -- is that accurate?

O'CONNOR: I work in technology and I have many, many children

and I feel overwhelmed with the choices and the lack of transparency about not just their online environment, but as you pointed out correctly, the devices in our daily lives, even the toys and what they can and cannot collect. And it doesn't necessarily matter that it's identifiable by name, if it's targeting you based on your habits and preferences and choices, that could close their worldview as opposed to open it up which is what we would hope the internet would do.

CASTOR: Thank you very much. I yield back.

SCHAKOWSKY: I now recognize ranking member of the Full

Committee, Mr. Walden for five minutes. I'm sorry? Oh, oh, I'm sorry, is that wrong? Okay, let me recognize Mr. Upton for five minutes.

UPTON: Thank you, Madam Chair. It is a delight to be here. I

know that Mr. Walden is at the other hearing. I think he intends to come back.

Ms. Zheng, I -- I think that we all recognize that the elephant in the room is truly -- we're going to have a system that's 40 or 50 with states or we're going to have one standard. What -- what is the -- what is the perception from the number of companies that you represent from the Business Roundtable in terms of how they would have to deal with maybe as many as 30 or 40 different standards as I would figure the number of states might join up with or team up with others, what -- what is the reaction to that?

ZHENG: Yeah. I -- we -- we...

UPTON: Goes along with...

ZHENG: I strongly believe that a fragmented sort of regulatory

environment where we pursue a state by state sort of regulatory approach to privacy makes for very inconsistent consumer protections. It also creates massive barriers to investment and innovation for companies that have to operate in all of these different states. It's simply unworkable.

And so that's why we think it's necessary to have a single national federal privacy law that preempts state laws. And I think the assumption that preemption weakens existing privacy protections is a false assumption. We strongly believe that a federal consumer privacy law should be strong and should provide additional protections for consumers that are consistent across every state in the country. As I think folks here mentioned earlier, devices, data, people, they constantly move across borders, across states. A state by state approach just simply doesn't work for this type of domain.

And in fact, even when you look at California's own privacy law, there is a rather strong preemption clause in the California law that preempts city, county, and municipality laws within the state of California and likely for the exact same reasons why a federal privacy law should preempt state laws.

UPTON: And are you aware, is anyone tracking what the other 49

states might be doing?

ZHENG: We -- we are. I think you are as well.

UPTON: Yeah, and are -- and any of those states getting close

to something like California is doing or are they -- I know it's a new legislative year for -- for many states, but what's your -- what's your thoughts on where other's place will be?

ZHENG: Yes. I think there are roughly about 30 different state

legislative proposals related to privacy. They all take -- many of them take very, very different approaches or regulate certain types of sectors, some of them are more general. Some of them may be focused on specific types of information that are personal. But what it demonstrates is that there is a ton of interest within the states and they're not taking a coherent, consistent approach.

UPTON: And what are your thoughts, do you think that any of

these things states will actually do anything yet this calendar year or not?

ZHENG: It's hard to say, but I think...

UPTON: Yeah, I know it is early.

ZHENG: I think it is highly, highly likely that a number of

states will pass privacy laws this year.

UPTON: And I know I don't have a lot of time left here as I ask

my last question, but I -- I thought that Mr. Grimaldi had some very good comments in his testimony about four different parts to achieve the goal.

One, to have clear prohibitions on a range of harmful and reasonable data collection, two is the new law should and distinguish between data practices that pose a threat to consumers and those that don't, three that the law should incentivize a strong and enforceable compliance and self-regulatory programs and finally, it should reduce consumer and business confusion by preempting the growing patchwork of state privacy laws.

As it relates to the first three knowing where I think I know where you all are a part for, where are you in terms of your thoughts as to those three first three principles, and maybe if we just go down the line. And we'll start it with Ms. Collins-Dexter as to whether she thinks that's a good idea or not briefly, knowing that I have a minute left.

COLLINS-DEXTER: Could you repeat that one more time? Apologies,

I was like taking various notes.

UPTON: All right. So Mr. Grimaldi had three -- four points of

which I think the first three that I'd like to focus on. One, that the clear -- have clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified by the

law, these are goals for the legislation, two, that the new law should distinguish between data practices that pose a threat to consumers and those that don't, and third that the law should incentivize a strong and enforceable compliance and self-regulatory programs.

So I guess now, we just have to go to yes or no with 20 seconds left.

COLLINS-DEXTER: Yes.

UPTON: Dr. Layton.

LAYTON: Yes.

UPTON: Zheng?

ZHENG: Yes.

UPTON: And Ms. O'Connor?

O'CONNOR: Yes.

UPTON: Okay.

O'CONNOR: But self-regulation alone is not going to be enough.

That was revolutionary in 1999, but it is no longer sufficient to protect consumers today.

UPTON: My time is expired. Thank you.

SCHAKOWSKY: I now recognize Mr. Veasey for five minutes.

VEASEY: All right. Thank you, Madam Chair. You know, earlier in

Ms. Collins-Dexter's testimony, something really concerned me and really hit home for me when she was talking about, you know, how poor people are being targeted for some of this marketing and -- and these privacy issues that we're having. And for a lot of the people that do fall within that category is going to be very important for them that these services remain "free" whatever free is. And of course we know that nothing is really free.

And what's so troubling about that is that in our society, obviously, we live in a -- in an economy that is based on -- on profit and -- and gain. What is the sweet spot? I just I would like to know maybe from Ms. Zheng or Mr. Grimaldi from a business standpoint what -- what -- what is the sweet spot? How can you still provide these services for free for the constituents that I represent and the -- and the people that Ms. Collins-Dexter was talking about, how do you preserve them being able to access this without them having to pay additional fees, but the market research and the other things that -- that go along with these services being free and -- and how do you combine all of that?

Is there -- is there a real sweet spot in all of this?

ZHENG: So I think -- thank you for that question, congressman.

It's a really important issue and I'm glad that you raised it and I'm glad that Ms. Collins-Dexter raised it. It's complex. It's requires additional attention. And there's significant technical, legal and ethical considerations as well, companies should not be using personal data about consumers to make discriminatory decisions in the areas of employment, housing, lending insurance or the provision of services.

But defining that line between using an algorithm to discriminate against consumers and using it to target, for example, ads in Spanish to Spanish-speaking consumers is challenging. So, we need to be mindful of some of the, these legitimate uses of certain demographic information that enable products and services to be better tailored to a consumer.

But we recognize that this is a really important issue as is the differential pricing issue that you raised. Although we have significant concerns with the particular approach taken in the California law, we welcome the opportunity to work with the committee on this issue and consider different proposals so, thank you.

VEASEY: For the areas where, I mean, for the areas where these

companies were trying to obviously maximize their return on investment where they need to control groups and run tests, can that still happen, Mr. Grimaldi, with more consumer protection and obviously the consumer protection is definitely needed. I think that you can just listen to just a very few minutes of today's testimony and realize that.

GRIMALDI: Correct. Congressman Veasey. I'm associating myself

with Denise's comments. We need to break apart any discriminatory practices from good practices. And you mentioned the value exchange that goes on behind consumers transacting their business

on the internet and Chairman Schakowsky went through a long list of what she has only done in the last 48 hours going to store, taking a flight, et cetera.

Those are useful practices that people come to accept. However, that information cannot be gamed for reasons of eligibility, of discrimination, of price discrimination, our industry is absolutely again that. There is a self-regulatory code that our companies adhere to in the Digital Advertising Alliance, a body that we stood up, stipulating to what Ms. O'Connor has said in that self-regulation the reason that we're here, we need help apart from self regulation.

We are here to partner with Congress to say it is past time, we are overdue in a national framework that speaks to these issues. But, yes, there are good uses. There are harmful uses. That's what we need to break apart and distinguish.

VEASEY: Madam Chair, I yield back. Thank you.

SCHAKOWSKY: I now recognize the ranking member of the Full

Committee, Mr. Walden.

WALDEN: Thank you, Madam Chair. And as you know we have another

hearing going on upstairs, so having to bounce back and forth.

In the United States, we currently enjoy an environment that allows small to medium-size companies to grow, to raise money and compete and in large part because they do not have to come to the government to get their business plans approved. We've successfully legislated based on well-defined risks and harms.

Dr. Layton, if data-sharing and privacy is regulated differently by individual states in the U.S., what will that do to the American marketplace?

LAYTON: So, assuming this could pass a court challenge because

I think it would violate the Commerce Clause as we discussed, I don't see how it's possible you can send products into other countries, I mean, into other states. If you are a retailer in Maine and you have to send your products to 50 different states and you have to set up 50 different ways to do it, I don't see why you'd start that business. I think you'd move to another industry.

WALDEN: So, how has GDPR impacted Google's market share in the

EU?

LAYTON: It has increased since it came into effect.

WALDEN: I think that's what we're showing right here on the

slide that nobody could read from afar I'm sure. Maybe we could put it on the big screen, take me off which would be a pleasant experience for everybody.

But I don't have a copy of that here at my desk. But I think what you're seeing here is that small innovators are actually leaving this space, right? And investment in small entrepreneurs is going down in Europe and going up in the United States since GDPR was put in place. Is that accurate.

LAYTON: Yes. So, this particular graph is looking at what's --

what they're highlighting here is the analytics competitors. So, Google Analytics is running in a lot of websites and depending on the company, they may have multiple competitors to Google Analytics.

Retailers have a set, different sorts of areas. So, essentially, some media companies, some larger firms are kicking off the smaller competitors for their -- they're kicking them off, so that means that those trackers have not been firing, that this is measuring.

WALDEN: Yes. My understanding it shows that shortly after GDPR

was implemented, Google's market share increased by almost a full percent and smaller ad tech firms suffered losses of anywhere from 18 percent to almost 32 percent. GDPR has proven to be anti-competitive and makes it more difficult for small businesses to compete and just one example of that negative impact.

Now, there may be other things going on affecting these numbers, I'll stipulate to that. But clearly, GDPR has had an effect.

Mr. Grimaldi, since GDPR has been in effect, academic research shows that investments in start-up companies in the U.S., in the EU, I'm sorry, have dropped by an aggregate of 40 percent -- 4-0. Compare that to the United States where in 2018 investments in start-ups neared $100 billion which

is the highest year since the dotcom boom, protecting consumers including protecting them from marketplace devoid of choices so they're forced to use certain products and services.

What should an American approach to data privacy look like that does not hamper small business and investment?

GRIMALDI: Thanks, chairman. You're correct. We are seeing that

falloff in Europe. And it is not because -- I listed some newspapers at the beginning that are not currently operating in Europe and it's not because they are not complying with the law and it's not because they are at fault; it is because they just can't afford that kind of a pivot to construct their services that could at legal risk, at great legal risk.

This is one of the many things that we are seeing with CCPA that is going to be a major deterrent if not a killing blow to American companies that can't deal with the labyrinthine construct of new regulations in California or other states that might force them to take down their online advertising funding regime for fear that they could be susceptible to a major lawsuit because they did not classify or categorize data in a way that could be returned to consumers because currently, these companies don't have those structures in place.

And now, in order to do something that, again, I stipulate was correct in its founding, transparency, choice, accountability is now potentially going to force companies to say we just can't afford to retrofit all of our systems and be able to collect that much data, and even if we do, there's a litigation risk that we wouldn't be able to swallow. So...

WALDEN: Could you put that litigation risk in common person's

terms? What are we talking about here if you're a small business.

GRIMALDI: Correct. Under CCPA, some of the provisions and we

are active as I think many in this room in dealing with the California Attorney General's Office, former Congressman Xavier Becerra being that Attorney General, he is taking a look at the current law and promulgating it to be enforced in January.

The litigation risk could mean that if a consumer requests their data from a company, if a consumer reaches out and says what do you have on me and how is it shared, the company has to be able to provide that in a certain timeframe and if it doesn't, it is in violation of the law. That litigation risk you can compound into the thousands or hundreds of thousands of requests that will multiply into the millions and billions of dollars. And that is something that smaller companies would not be able to deal with.

WALDEN: My time has expired. I thank all of our witnesses for

enlightening us on this issue. Thank you.

SCHAKOWSKY: And now, I yield to the chairman of the Full

Committee, Mr. Pallone.

PALLONE: Thank you, Madam Chair. I wanted to build on your

questions. Some uses of our data are certainly concerning. This committee has explored many of them. Cambridge Analytica's use of people's data to manipulate their political opinions and influence the votes, for example. And we had hearings with Equifax, Facebook and Twitter, which began to reveal just how little we all know about who's collecting our data or what they're actually collecting.

And I think many of us have this vague idea that everyone is collecting everything and that there's nothing we can do about it. But in my opinion, that's not acceptable because some data maybe just shouldn't be collected at all.

So, in that vein, I want to ask Ms. O'Connor, data collection has become extremely profitable, leading some companies to collect every bit of data they can but is there a line that shouldn't be crossed? Should there be some limits on actual collection?

O'CONNOR: It would be our position that yes, at least as to the

most sensitive information there should be very clear notices and an awareness on the part of the consumer. Again, the example I used of my fingerprint and my phone being collected for one purpose, not being used for any other.

When I use a map app, they obviously need to know my location . I do not want that location sold or transferred. Are there types of data that shouldn't be collected at all? In our bill, in our proposal, we looked very seriously at issues of precise geolocation, biometric information, children's data, content of communications and health information as deserving higher sensitivity and higher protections.

PALLONE: All right. Let me ask Ms. Collins-Dexter, how do you

think we should be -- well, how should we be thinking about limits on collection and what about limits on sharing, sharing with or selling to third parties?

COLLINS-DEXTER: I echo Ms. O'Connor. I think we should be

looking at all of this right now. Companies have financial incentive to collect as much information as they can and store it forever with no obligation not to do that.

I think we have to have meaningful data minimization requirements. I think we have to definitely look at the various ways in which information is often used as a proxy for race. So, for example, we know that Facebook and a lot of big tech companies actually don't collect explicitly race data. However, many things around geolocation and daily habits are able to like to put together this data profile, in which like people are able to ascertain that it's used for predatory marketing practices.

And so, we have to be able to like parse through all of that information and keep a constant eye on impact, which I think should be at the core of any legislation that we're looking at.

PALLONE: Thank you.

Ms. O'Connor, what about limits on sharing with or selling to third parties?

O'CONNOR: Absolutely. We would put this in two separate

buckets. First, limits on sharing, again, for the most highly sensitive of the categories I mentioned, particularly things that are immutable or most intimate about you. On selling, we would also put limitations or sharing with third parties that the third parties would have to be bound by whatever promises the first party made about that data. So, absolutely, we look very hard and limit secondary use and third party sharing.

PALLONE: Thank you. I just want to ask about limits on sharing

people's information with affiliates because we know that many corporations own multiple affiliated companies that the average person would not contact, like YouTube, Android and DoubleClick are all owned by Google or Jet.com and Sam's Club both owned by Walmart. Data collectors say they don't sell data to third parties may still want to share that with their affiliates.

So, let me ask Ms. Collins-Dexter, should there be limits on sharing people's information with these corporate affiliates?

COLLINS-DEXTER: Yes, absolutely. We should definitely be

looking at how these third party companies are operating as we saw with Facebook last week as we continue to see with as you all have mentioned Cambridge Analytica and others. You have these third party data mining companies that aren't regulated, aren't looked at, they're gathering data, scraping it and selling it to companies for predatory marketing purposes, selling them to like law enforcement without our consent and because we don't even know that these companies are looming in the background. It really even further limits our choice or ability to say no.

PALLONE: And just quickly, Mr. Grimaldi, behavioral advertising

needs data to target ads at the most appropriate audiences. How would limitations on the collection and retention affect your member companies? Are there limits that can be established or legislation that provide reasonable protections to consumers that your member companies would accept?

GRIMALDI: Thank you. We currently have a very robust

self-regulatory program that is targeted to consumers having transparency into their online behavioral advertising and the ability to click through the ad via icon in the upper right corner of every ad, it's served over a trillion times per month that takes you to a page that says why am I seeing this ad and how can I stop seeing it.

There is tremendous uptake in terms of people going through that ad up to the tune of about 70 to 80 million unique impressions. So, we offer that control. One of the messages today before you is, as much as we are trying to educate consumers on that, there is still a need for a federal program that can help us distinguish what kind of advertising is working. What is considered harmful and what do consumers need to know, again, before they click on something.

It could be something that is very much tailored to what they are looking for, an ad that speaks to them. We have much resource that shows the consumers prefer targeted behavioral advertising rather than generic advertising. But we want to make sure consumers have those controls so that they can stop seeing those ads. And, again, that could be enshrined.

PALLONE: Thank you.

SCHAKOWSKY: And now, I yield to Mr. Latta, the former chair of

this subcommittee and my friend.

LATTA: Well, thank you very much.

If I could ask just a quick point of personal privilege and congratulate the chair on assuming the gavel so congratulations. It's a great Subcommittee. And, Madam Chair, before I begin I'd also like unanimous consent and enter into the record excerpts from the WHOIS report from the Department of Justice attorney general, cyber security task force.

SCHAKOWSKY: Without objection so ordered.

LATTA: Thank you, Madam Chair. If I could reclaim about 30

seconds there.

Last Congress, the Energy and Commerce Committee held nearly a dozen hearings discussing privacy and security issues that includes much-publicized hearings where we heard from the CEOs of Facebook and Twitter about how the companies collect, safeguard and use data.

From those hearings, it was clear that while these companies provide a service that Americans like, consumers aren't always clear about what happens with their personal information. With the California law slated to take effect at the beginning of next year, time is of the essence, in a divided government, it's not always easy to tackle the tough problems but I believe the time is right to work together on a federal data privacy solution.

Both consumer groups and business organizations have come on board in calling for a national standard. We all agree that consumers should have transparency and accountability and we want to ensure that the United States stays the prime location for innovation and technology.

Dr. Layton, if I could ask you I've been hearing from many groups regarding the loss of access to information about domain name registration or the WHOIS data and the role it plays in protecting consumers. Would you explain how WHOIS increases online transparency so that consumers may have a better understanding of who they're interacting with online?

LAYTON: Right . So, the WHOIS database for just a lack of a

better way would be a sort of address book for the internet, who is registered, who owns what particular domain.

LATTA: And following up, would you want to comment on how the

GDPR is creating challenges to accessing that data?

LAYTON: Absolutely. So, one of the key problems is that because

of its ability to retract information that the domain name registers are masking their identity. This is making it very difficult for law enforcement to find out perpetrators of crimes.

It's also an issue, too, if you need to contact, things with intellectual property, for example. So, there are many concerns with this and this reflects our historical view of privacy, of prioritizing the right to know. We believe that the public has a right to know about these things.

LATTA: Could you add a little more depth about how that

information helps in identifying those bad actors and those criminals that are out there and help that law enforcement needs to find those individuals and bad actors?

LAYTON: Right. Well, in just the same way that if you looked at

a phonebook and you would see well, a certain address in this place, who lives at that address, I mean, that is the key function of law enforcement. So, if you're taking that away for the internet for global, for law enforcement everywhere, that's a serious problem.

LATTA: And please list your top three concerns for the GDPR and

also the CCPA which is the California law?

LAYTON: Sure. Well, I'd say the first concern from the U.S.

perspective would be First Amendment, free speech concerns. The level of government requirements is so high that it reduces (ph)

expression, that would be number one. But certainly safety would be number two with regard to just what you described.

You have other issues with people who have committed crimes in the European Union who are asking that their records be erased or removed, that have committed murders, child molestation and so, that's a serious problem.

And I would say thirdly, the sort of the dumbing down of consumers, that there's creating a false sense of security that somehow that regulators have to answer what to do, it doesn't allow consumers to take responsibility for when they go online.

And I would add number four which is I think that you're freezing in place technology, don't let them evolve. So, for example, the EU will require using certain kinds of data protection technologies, but we can actually make them better. So, if you require a company to do technology A today, I can invent technology B tomorrow and I'm not allowed to upgrade to it. So, that's a major problem as well.

LATTA: All right. I appreciate it. Thank you very much and I

yield back the balance of my time.

SCHAKOWSKY: Next will be Mr. Lujan, New Mexico.

LUJAN: Thank you very much, Mr. Chairman, for this important

hearing. Let me to jump into this. In 2000, the FTC recommended that Congress enact consumer internet privacy legislation. That was 19 years ago.

The Subcommittee held a hearing after the Equifax breach in October, 2017. We had Mark Zuckerberg before the full committee in April 2018. The 115th and previous Congresses failed to pass meaningful privacy protection even though there were commitments made to the American people.

So as we jump into this, Ms. O'Connor, an entire economy based on data has been built. But we didn't stop to consider the risks and potential downsides, companies collecting data have put consumers at risk.

Mr. Grimaldi, in your testimony, you say that the law should incentivize strong and enforceable compliance and self-regulatory programs by creating a safe harbor process, but I'm concerned that incentives won't be -- we need some accountability.

So, one of the ideas that we have is to require companies to conduct risk assessments. If you want to process data for consumer-related usage, you need to assess the foreseeable risks of such uses.

So, Ms. O'Connor, yes or no, should we require risk assessments so companies factor the risk and potential harms in their decision-making?

O'CONNOR: Certainly, the concept of risk assessments are

privacy impact assessment has been around since even before those FTC hearings, which I attended in the year 2000 and before.

And certainly, that's part of a robust privacy compliance program. But we do want to be mindful of that burden on small businesses and make sure that the legislation that is comprehensive is elegant and efficient. It's simple. It's streamlined and easy for a small, a medium and a large company to know what the rules are and to abide by them.

So while I'm certainly in favor and I have implemented a number of PIAs or risk assessments in my time in the government and in the private sector, I want to make sure that the law is simple and clear for consumers and for companies.

LUJAN: So assuming the same disclaimer holds true to the next

question, yes or no, should we require a privacy protection officer at companies that collect large amounts of data who would be responsible for training staff, conducting audits, working with authorities and advocating for privacy with the entity?

O'CONNOR: Yes.

LUJAN: There is a great editorial that was authored in Forbes,

January 15, 2019, entitled "2019 Data Privacy Wish List, Moving From Compliance To Concern." I'd ask a unanimous consent to submit it into the record.

SCHAKOWSKY: Without objection.

LUJAN: In it, one of the points that was made here is from a

move from privacy compliance to concern and care, that rather a philosophy that treats data with extreme care and with prevention of data breaches in mind that that something that company should be doing. So that's where I'm thoughtful from an incentive perspective of what we must be doing going forward.

Ms. Collins-Dexter, you highlighted in your testimony some important aspects here. And I'm concerned about implications for access to housing, lending, digital redlining and voter suppression as we talked about information that is shared that is sensitive. Would you agree that this is a problem?

COLLINS-DEXTER: Yes. I absolutely do.

LUJAN: Have companies responded when it's been brought to their

attention that their products or services are having discriminatory effects?

COLLINS-DEXTER: On the whole, no, it has not. We've sat at the

table, part of our model is a corporate accountability model, which requires direct engagement and negotiation. We've sat them, in the companies, Facebook included for many years and have a lot of discussions with them.

And for every policy they develop we tend to find weeks, days, months later that the problem is really much larger than what was initially indicated. And so self-regulation has not proven to be a viable option.

LUJAN: So with that being said have the responses from industry

been adequate in this space?

COLLINS-DEXTER: Have the responses from the industry?

LUJAN: Been adequate?

COLLINS-DEXTER: No.

LUJAN: Are there changes the companies have made voluntarily

that should be made into law? And we can get into the details, just yes or no.

COLLINS-DEXTER: Yes.

LUJAN: So, we'd be happy to work with you in that space.

Mr. Grimaldi, the IAB represents over 650 media and technology companies that together account for 86 percent of online advertising in the U.S. You heard the quote that I referenced from this editorial. Are these companies looking to protect my privacy when they're making this business decisions?

GRIMALDI: Congressman, they are. They are, without a doubt. One

of the things, again, why we are here today is to ask government to fill in those holes that we can't fill in. Should there be mandatory components of a privacy policy that does not let a user accidentally click something to give consent.

Is there -- are there pieces where we could work with you on strengthening what we already have put in the market for consumer controls.

LUJAN: Let me ask a question as my time expires, and I'll be

happy to submit that to the record. We can get a response. Would you agree that companies need to shift to a philosophy that treats data with extreme care with prevention of data breaches in mind?

GRIMALDI: I think there -- I think what needs to be defined are

those unreasonable and reasonable uses of data. Again, many on the committee have said, we use data -- we give our data to a certain aps or to a certain programs to help us every day.

Is that data being used for those purposes? Are there harmful uses of data? I think the absolute answer is yes. Are there guardrails we can put around it, more self-regulation, more partnership? Yes.

LUJAN: Madam Chair, just as my time has expired, I thank you

for the latitude here.

It just seems that we wouldn't be here today if, in fact, there was an effort to concern and care versus just compliance. And I think that's what we're looking for, is how can we work on this collectively and together such that we get to that point. So, I appreciate that time.

Thank you, Madam Chair.

SCHAKOWSKY: I recognize for five minutes, Congressman Bucshon.

BUSHON: Thank you, Madam Chairwoman.

I was a healthcare provider before and health information is some of the most sensitive information that's out there and it's also some of the most valuable. So, I hope that whatever we do here in Congress specifically addresses health information, because it's really critical and important.

As you may have heard, last week it was revealed that Google's Nest Guard home security device had a microphone inside the device that consumers did not know about and it was not disclosed.

As I have discussed in prior hearings on data privacy, including with Mr. Zuckerberg, I'm concerned about the inappropriate collection of audio data. And it seems that everyone denies that that happens, but I think everyone knows that it probably does.

So, Ms. Zheng, can you expand on how the right to privacy would play into this type of practice, and how we would deal with that?

ZHENG: Yes. I think -- thank you for that question,

congressman. When it comes to audio data, if it is personally identifiable information or personal information, it falls within the scope of a privacy -- new privacy bill. I certainly believe that transparency, control, access the right to correct it, the right to delete it should be right the consumers should have, including for audio data.

BUSCHON: Because that's going to be important because if we

exclude things that you actually type on the internet, but we don't have the things in privacy where if you're talking your phone picks it up and send a keyword to someone and they advertise based on that, then we're missing the boat on that.

I want to prevent collection of data without consumers' knowledge and audio data would be there. And Dr. Layton, do current laws cover this type of omission from Google about a microphone?

And second, if we decide to grant additional authority to the FTC would you have any suggestions on how the FTC may play a role in addressing intrusive data collection policies with -- including audio data without harming innovation?

LAYTON: Thank you, congressman. I think it's excellent that you

raised the point when you use the various devices in your home, Alexa home and so on, you're having conversations with your family members.

And I think law enforcement has actually used some of that data in some cases and have good purposes for it, actually. In terms of the Federal Trade Commission they are engaged in this process now. I don't know if audio is a specific part of their inquiry. I would have to get back to you on that. I can't recall at this moment.

BUCSHON: Okay.

LAYTON: But I don't see from a technical perspective why audio

would be different, because it would be recorded as the same data even though you're speaking it would be transcribed into a data file, so...

BUCSHON: Okay. The other thing I want to quickly say, then I

have a question for Mr. Grimaldi is that also, we need to address hardware as part of this not just an app, but hardware because data -- location data is really important.

And there was a local news media here in town who turned off their phone and did everything they could except take the battery out. Went all over the city of D.C. and then went back, plugged it in and all the metadata everywhere they were was recorded.

And as soon as they turned that phone on, it all went out to the internet. So, I hopefully, anything we do on privacy also includes hardware, not just apps, not just software. That would be important.

So, Mr. Grimaldi, in your testimony, you highlight that data-driven advertising has helped power the growth of the internet by delivering innovative tools and services to consumers.

Many constituents, including myself and I'm going along the audio theme here, have concerns about how conversations when not directly using an app, device or other electronic device appear and then later online ad based on keywords in the conversation. Can you help me understand how this is happening?

GRIMALDI: Sure. There is -- and also, I think it's important to

understand the difference between personal data and synonymized data. And that is if you are using -- if you are in your conversation using words that were flagged that weren't Congressman Bucshon, but they were an individual who was into hunting or was into automotive, cars, you name it, sports. That data could be tagged for you and used to serve you better targeted ads.

BUCSHON: Can I just interrupt for a second? So, I was having a

conversation with my communications director. This happened about a month ago, talking about a certain subject. And the next day he got ads on his computer, specifically about that particular subject.

We happened to be talking about tennis because he's a tennis instructor, but nonetheless, so. Continue.

GRIMALDI: Right. Without intimate knowledge of how that

hardware is constructed. If I were to take that as an example of just your web browsing, those sorts of things could be flagged in order to serve you ads that are not generic, that are more tailored to your interest and done in a way that, again, that the word synonymized meaning there is -- you are put into a category rather than your name, your address, your Social Security number but just your likes and dislikes.

And then that enters a marketplace behind the web where that information is used to serve you better ads without linking you personally to your information, your intimate information. It's another piece of that reasonable and unreasonable construct we're talking about.

BUCSHON: Okay. My time has expired, but I want to make sure

that whatever we do here in this committee and it includes audio data and also considers location data based on hardware within a device. Thank you very much. I yield back.

SCHAKOWSKY: I recognize Congressman Rochester.

ROCHESTER: Thank you, Madam Chairwoman, and thank you so much

for setting the tone of this hearing and this is a vitally important topic for Delawareans but also for our nation.

And I want to thank the panel as well. More and more in our daily activities they involve the use of the internet. Many of us pay our bills, shop, play games and keep in contact with friends and relatives through websites or online applications.

However, with all of these activities taking place online, websites are amassing more and more personal information. This presents serious privacy concerns. Large scale data breaches are becoming more common.

And consumers have a right to know what is being collected, how it is being used and should be notified when a breach has occurred. Most of you on the panel today have discussed the need to give consumers more control over their own information. To get more control over their own information and should it be -- how it should be collected and how it should be used.

And I want to drill down just a little bit deeper on that and ask Ms. Zheng, the Business Roundtable's privacy framework promotes the idea of giving the right to access the correct and correct inaccuracies in the information collected about them.

So, can you talk a little bit about what you mean by information collected about them? And does that just refer to data points collected or does it also include any inferences made based on that data?

ZHENG: Congressman, that's a good question. And it's a very

specific and detailed question and to be honest with you, we still need to discuss within our membership. Right now as we drafted our proposal, our framework, the right to access, correct and delete your data does apply to your actual personal data. So, but to answer your further question, I would need to follow up with you.

ROCHESTER: And I'm going to ask a few other people questions

around this as well. I mean I think a lot of us are familiar with the story of the individual at Target who got the coupons, came to the father's house for a pregnant teen and again, it was inferences.

And so, I want to ask Ms. Collins-Dexter, what are your thoughts on access and correction and should consumers be able to see and correct inaccurate inferences made about them? And I want to start with you.

COLLINS-DEXTER: Yes. Absolutely. We think that people should

similar to a credit report have an opportunity to challenge and correct information. One of the things that we've even seen with some of our work around voting records and purges that have happened across the country is that there is a lot of data collected.

And based on like inaccurate names or misspelled names that it allow for voters to be purged from files across the country. I think as we think about all of the various data points and all of the mistakes that happen, again, we are finding the people that tend to be most impacted are low income communities, of people of color, people who aren't able to actively challenge and correct the record on themselves.

So, I would say it is extremely important in a number of different fronts that we are allowed to do that, and any privacy legislation should allow for that.

ROCHESTER: Thank you.

And Mr. Grimaldi, you didn't really talk about consumer's right to access and correct information collected in your testimony, but how do you think giving those rights to consumers would affect your member companies?

GRIMALDI: Thanks, congresswoman.

To echo with some of my co-panelists have said. Consumers have a right to delete their data. And I think that there is -- there are things to explore with those rights. They are obviously fraud, misuse, other components that could negatively affect either a consumer's online experience or their just life experience.

And we're seeing that contemplated in Europe. And we're seeing that contemplated in California. There are problems though, I would point out, that could come about when consumers request their data to be deleted and the authentication of those consumers requesting it.

One of the major pitfalls that we're currently working on with the California law is if somebody can have their data deleted, how do they authenticate themselves to make sure it's them? If somebody can request their data, how do we know it's them and it's not somebody stalking them or somebody meaning to do them harm? These are really important questions.

ROCHESTER: Right, right. I want to kind of close out my comment

by just saying that why this is so important is because I think a lot of people do feel that it's fait accompli, this is world that we now live in.

And that's really what the role of Congress is, is to make sure consumer protection going back to what our chairwoman said. Thank you so much. My has expired.

SCHAKOWSKY: I now recognize for five minutes, Congressman

Carter.

CARTER: Thank you very much, Madam Chair, and thank all of you

for being here. This is an extremely important subject. And we want to do the right thing, so that's why we got you here. You're the expert. You're the ones that we want to learn from and hopefully build upon.

Dr. Layton, I want to start with you. First of all, earlier, one my colleagues mentioned the WHOIS database. Can you explain that very briefly what that is exactly? It's...

LAYTON: Well, I just used the address book for the internet.

Those are registering the names that they have to disclose who they are.

CARTER: Well, it's clear through your testimony as well as your

background that you have a good grasp of GDPR and the impact that it's had. It's my understanding that the WHOIS are (inaudible) and it's the governing agency over WHOIS that they have -- that they're actually run into problems with this and they've actually said that they're not going to be collecting that data anymore.

LAYTON: So, no, they've actually, for some -- for quite a long

-- I think at least a year they have been trying to work with the officials in the European Union to

highlight to them the problems and to find a resolution and the pressure from the extreme privacy advocates in the European Union are not letting them come to resolution.

So as I understand today, I'm not -- I don't have the most up-to-date, but I think there is an impasse right now because it's not resolved. And the -- so the information is not available.

CARTER: Well, this is the kind of thing that we want tol learn

from, I mean, we don't want to make the same kind of mistake that obviously they've made and because it's my understanding that WHOIS data is very important, particularly to law enforcement. Has that been your experience?

LAYTON: Yes. Well, absolutely. I mean, it's a major issue for

law enforcement, intellectual property rights holders. People in the public who may need to do research and so on. I think the lesson learned here is we've heard before the way to hell is paved with good intentions.

I think everyone has had good intentions. And they've overreached. They went too far. They didn't have a process to test the various provisions. Everybody got to tack on what they thought made sense and then they just bring it over the finish line and we have to live with it.

CARTER: What do you think we could learn from that? I mean, how

could we make it better?

LAYTON: Well, at least one of the things I would say in terms

of how we are ahead in this respect. In the United States, we have a transparent policy process. When we are submitting anything to the Federal Trade Commission as part of what they're doing, you have to disclose your name, who you are when you're conducting this hearing today. The policy process now in the EU because of this rule means you can mask your identity. So you can submit into a regulatory hearing. You don't have to say your name. You don't have to say who you are for privacy reasons.

So, what I would encourage Congress to do is to keep with our tradition for the public's right to know, to continue in this vein as you're having the hearings today. And to take these steps to look at where it hasn't worked and to not make the same mistakes.

CARTER: Let me move on. Earlier, we talked about market share,

particularly as some of the companies in Europe have grown in market share and at the expense of others as a result of the GDPR. What's the primary reason for the change in market share for some of these companies?

LAYTON: So the - well, in many respects there are - it's

because the number of firms have exited the market, they are - they've decided they're no longer going to operate. So in many respects that the advertising market has shrunk in the sense that there are few properties on which to conduct advertising, that would be one thing. The other issue is that when those other smaller players leave, it just means that people visit the larger players more.

CARTER: What - has this had an impact - obviously it's

had an impact on the - on the exports, Europe, of various content in digital goods?

LAYTON: Right. Well, so for me when I'm sitting in my office in

Copenhagen, I try to go to Chicago Tribune, I cannot open it. I just a white paper that says, "Sorry we're not delivering our content." And, you know, that's unfortunate for me. I can't see the information. It's too bad for the advertiser. They can't put the advertisements on the page. It's sad for the one million Americans who live in the EU.

CARTER: I was about to say it had - obviously it has an

impact on them and they're not able to get the information.

LAYTON: Right. So I think as Mr. Grimaldi - he pointed out

very well and I think his testimony makes it very clear, it's not that they don't want to do it, but it costs too much money and there is a regulatory uncertainty. The legal risk is so high because it's not just - it's so new these rules, we don't know how they'll be interpreted and it's a whole value

chain that all of the partners who might be working with Chicago Tribune or whomever may also be liable.

CARTER: Well...

LAYTON: So they don't want to take the risk.

CARTER: Again, I want to thank all of you for being here. I

think there are important lessons that we can learn from the experiences both in the European -- European Union as well as what we're trying to do in California. Obviously, what we don't need is 50 different sets of rules governing. We need one set of rules here in America and hopefully - and I've already said, I don't want to stifle innovation, so that's one thing I hope we keep in mind in this committee as we move forward. Thank you, Madam Chair, and I yield back.

SCHAKOWSKY: Thank you. And now I welcome the vice chair of this

committee, Mr. Cardenas.

CARDENAS: Thank you very much, Madam Chair. And thank you for

holding this very important matter before the public. And to the ranking member as well, thank you. Miss O'Connor, would you like to shed maybe a little bit of light on the dialogue that you just witnessed over the last three or minutes about the EU and maybe the mistakes they made and the things that we could learn and the cross-reference between innovation and privacy?

O'CONNOR: Thank you so much, sir. I think it's fairly certain

that we in the United States will pass a United States law that reflects our values and our cultural traditions and our unique opportunity here as the birthplace of Silicon Valley, but I think there also are shared values, values of respect and dignity, values of customer trust that our companies, our US-bred companies can certainly adhere to.

I think privacy and security are a form of corporate social responsibility in the digital age and are essential to doing business in a thriving U.S. economy and around the world. Yes, it is important to get to a federal standard, but it's important that that standard be strong and be understandable by small, medium and large enterprises in the United States.

And most importantly, be one that customers can trust, that consumers and citizens of this country can have certainty that their information is being treated fairly, that they are not being discriminated against, and that they understand the consequences of the bargains that they strike with companies.

CARDENAS: Well, one thing that I enjoy the most is being able

to go back to my district and I'm blessed that my two grandchildren live in my district, so I can drive five minutes, jump on the carpet, roll around with them and play with them and know that when they grab a toy like my six-month-old, she's at that age where everything goes in her mouth, know that consumer protection is something that we take for granted in this country.

We didn't do that back in the day maybe decades ago, but at least today I know that there's a 99.999 percent chance that that is not going to hurt my little granddaughter. Speaking of children, under the CCPA, businesses are supposed to provide an opt-in mechanism for children 16 and under to allow companies to sell their personal information as defined by the CCPA. How do they know whether the children are 16 and under under any system?

O'CONNOR: Well, that's such a great point, because it

requires more authentication and more knowledge in order to know who your consumer is. I think you've identified one of the very compelling gaps in our coverage right now, the above COPPA but below majority age group in our country. I have several of those people living in my house right now and they are a challenging on the internet to say the least. And it certainly bears consideration of what we should do going forward to consider whether COPPA is working adequately and what to do with that in between age group.

CARDENAS: What's the mechanism for - to get parental

consent for children under 13?

O'CONNOR: It's somewhat complicated and requires several

steps of the parent self-authenticating and providing phone numbers or email addresses or the like. I seem to do this every single day on my computer for my youngest child. But it's still is fraught with

some peril that the child may be providing inaccurate information or that they - the data may be used in a way that is unanticipated by the parent or the child.

CARDENAS: Under the federal law, COPPA, companies must obtain

parental consent before collecting personal information online from children under the age of 13. How do companies verify parental consent and how does the FEC enforce this?

O'CONNOR: They - parent often has to respond to an email

verifying that they are the parent or that they have authorization. The FTC (ph) has taken some cases and I think there is concern in the - in the marketplace about whether the enforcement mechanisms have really fully grasped the complexity of the issue both in the online world and as you point out in the internet of Things world.

CARDENAS: What seems to be logic or the history on the

difference between a 12-year-old and a 13-year-old and why is that the cut-off point?

O'CONNOR: I'm sorry I can't speak to the legislative history on

why that number. It certainly is one that bears a relevance in the number of cultural traditions, but I think we all know that one 13-year-old is not the same another in many households and there's a large age group between, again, 13 and 18 that we should thinking about as well.

CARDENAS: How do we expect the 13-year-old to do - wade

through this without parental consent or somebody - an adult helping them?

O'CONNOR: I totally agree. I think kids, teenagers, and

grown-ups in this country deserve greater supports and protections around their personal data online and off.

CARDENAS: I think it would be naive for us to believe that

there isn't a motivation out there with largest corporations in the world and getting more dominant and larger for them not to look at our children as consumers. If you look at the bandwidth of a consumer power of a teenager and a 20 some year old, a 30 some year old, et cetera, there's tremendous motivation for individuals to abuse the information of our children and I think it's important that - thank you for the confidence you gave that you believe that Congress (inaudible) going to pass something. I hope that we do. Thank you for that confidence. I yield back.

SCHAKOWSKY: Now, I yield five minutes to Mr. Gianforte.

GIANFORTE: Thank you. And first, I'd like to thank the

chairwoman and ranking member for welcoming me to this committee. Thank you. I look forward to serving. And I'm encouraged by the conversation today. I think there's some good bipartisan common ground here to find solutions.

The internet has removed geographic barriers for many of our rural areas that previously prevented small companies in rural towns from competing globally. Concerns about data misuse are warranted but creating an over burdensome regulatory environment would have devastating effects for this coming new prosperity we're seeing in rural America.

I think we all agree. We've heard the testimony today that consumer data must be secured. And that we need more transparency and accountability in all of our practices and we need a national standard. Our job is to find a balance between these overly prescriptive laws like GDPR and - versus a patchwork of 50 different laws in different states.

Trying to comply with either would devastate small businesses. We've heard that in the testimony today. While increasing market share for some of the largest companies we see. And this is what's caused the concern. The burdensome top down approach taken by GDPR can stifle innovation and lead to less information simply because it's too costly to comply.

It's imperative then we adopt one national standard and that clearly defines the responsibilities of consumers and businesses and I think we have unanimity on the panel today, so I appreciate that. Consumer concerns over their data can be attributed back to a lack of transparency and misunderstanding of how their information is being collected and used.

Bad actors should be punished. We've seen many of them pursued by the FTC and also through the loss of consumer confidence. The market tends to enter in here. In our internet business, my wife and I started in our home. It - over 15 years, it grew to one of the top 100 websites in the world.

We had about eight million consumers a day and we were entrusted with the data for nearly 2,000 organizations around the world.

Protecting customer data was paramount in our business. We knew that the safety of our customers' data, which we protected in the cloud was the key to continued viability of our business. The stakes and the consequences could not have been higher. We had to protect our customer data or face going out of business.

It's difficult to regulate a dynamic industry and hastily rushing to draft legislation could have more unintended consequences than solutions. We've seen that in GDPR in the California rights. As debate over consumer protection continues, we should pursue one national standard that increases transparency and accountability while protecting small business and innovation.

I have a couple questions. Dr. Layton, with all of this in mind and in light of the light regulatory touch we've taken in the US historically, can you please discuss what you believe are the best way to guard against entrenching larger companies and disadvantaging smaller business?

LAYTON: Well, two words, permission-less innovation. I mean I

think that that's been one of the most important things about economy was that we allowed organizations - we allowed companies to try. People - just you yourself, you didn't have to - I don't - I doubt that you went to Washington and say, "May I try this website?" And you just got going.

GIANFORTE: Yes. Okay. Thank you. And, Mr. Grimaldi, we heard

from Ms. O'Connor in her litany of 260 applications, very impressive, and the near - the intractability of complying with them all. I mean your testimony, I thought it was very helpful, you recommended moving from these closures and check boxes to prohibited practices. Can you give us a couple of examples of prohibited practices that you'd put on that list if we were to draft legislation with that approach?

GRIMALDI: Sure. Thank you, Congressman. I think Ms.

Collins-Dexter has an unbelievable list in her testimony. Eligibility -- improper targeting because of eligibility and discrimination. The use of sensitive information which would be - need to be defined, we've spoken a lot about it today. The consumers don't anticipate and would never want to share or would never want to be used. I would say even if it is synonymized and not linked to their personal - their personal - their data along the lines of healthcare providers or addresses and such. I think that's all important.

GIANFORTE: Do we need to differentiate between the types of

data that's being collected and how would you suggest we do that?

GRIMALDI: Absolutely. I think that's - again, Europe should

not dictate what our national law should be. I don't think one state should either. I think this body and the Senate is the best representation of what consumer sentiment is around these issues. My industry needs trust or else we don't have people logging on to our websites. We don't have people clicking on our ads. The whole internet economy is built on that. These are the things - these the important conversations.

GIANFORTE: Okay. Thank you. I want to thank the panel for your

testimony today. It's very helpful. and with that, I yield back.

SCHAKOWSKY: And now, a belated happy birthday and I call for

five minutes on Mr. Soto.

SOTO: Thank you, Madam Chairwoman. I believe most Americans

have a basic understanding that their personal data is being used, but there are certain expectations of privacy that I think are reasonable for users to be able to have throughout the United States, that their personal data be kept secure and not be stolen in a cyber-breach, that their personal health data be protected so that it couldn't just be acquired without their permission or that we avoid a society where government monitors all of our data in some Big Brother type of situation that we're seeing now in China and in Russia.

You know, we've heard some complaints about states getting involved in this and the Supreme Court has gotten involved in it which I'll get into in a second. Really the internet is a part of the interstate commerce but it's this committee's lack of action in legislating that has created this vacuum for states to act.

First, I want to just point out that the Supreme Court (inaudible) we have some right to privacy for our personal data. In the recent Carpenter v US case, they at least applied the fourth - government cannot get personal data from cell phones without a warrant and I wouldn't be surprised if by five, four majority or more that that's extended to other rights.

So the Supreme Court is already acting. States have already stepped up. There's been a lot of talk first about a duty of care. That has mostly been in the purview of academia but it's something that we ought to consider. Cyber security protections, properties of data consistent with disclosures and handling requests and complaints for use of data. A second big issue we saw Delaware tackle with requiring privacy with requiring privacy policies to be conspicuously available on websites. I don't think that's much to ask since we have that for a lot of contracts.

And then, thirdly is really sort of the big question now on privacy in general. California passed the Consumer Privacy Act of 2018 where there's a right to request businesses disclose data collected, right to request businesses delete personal information, and then the right to opt-out without being discriminated against, and I think that's the multi-trillion dollar question in the room today. That's where I want to start by asking our panel.

Starting with Ms. O'Connor, do you think that you should be able to opt-out of these sites' ability to collect data without being discriminated against, basically denied use of service?

O'CONNOR: Certainly. And as I mentioned before, there's a

primary purpose in a primary data collection for the transaction. So, to send me the book or the (inaudible), you have to know my address. But I do think individual consumers deserve more not only agency, but control over their data and the data life cycle to access, correct, and delete data if they want to as well.

GIANFORTE: Thank you for your input.

And, Ms. Collins-Dexter, do you think you should be able to opt-out without discrimination?

COLLINS-DEXTER: Yes. I think opt-in forces -- well, rather, I

think when you set an opt-in framework, it forces companies to make the case for why data is needed for desired use and why consumers should consent to that.

I think, however, even in an opt-in framework, I think as we've heard examples over the day, companies will do all sorts of tricky things to get consumers to consent the things that they want to do, and so I think legislation has to really move beyond the choice framework and really focus on prohibiting harmful use of data, establishing baseline norms and obligations such as data minimization and purpose implementation.

GIANFORTE: Thank you.

And trying innovation on this aspect, Ms. Zheng, do you think it'd be a viable alternative that people can charge a user fee should they want to opt-out of data collection? Would that still embrace the kind of innovation that you've been talking about?

ZHENG: Thank you for that question. I think if that companies

choose to do that or choose to adopt that approach, that would make sense, but I'm not sure that mandating it in statute would make any sense. It would certainly hurt innovation.

GIANFORTE: And, Mr. Grimaldi, on this sort of choice, should

you be able to opt-out without discrimination or would it be appropriate to potentially charge the user fee in the alternative or deny or a service altogether?

GRIMALDI: Thanks. A couple of things, we see that not in terms

of data for shopping data for other use, but we see that in terms of just the value of exchange on if you want to access to certain subscription website and view their content, you have to pay a fee. That's that value of exchange.

To your question of should you be able to opt-out and not receive those services, I think that's another thing that we need serious contemplation because I don't think a "one fits all" approach would work here just in terms of that being a defined right and the massive disruption that could cause to websites, large, small, Google, Amazon, a small yogurt shop, if you opt-out of giving your data, can these companies survive where they're monetizing it, in a way that a consumer knows about that. It has that policy interface or the opt-out mechanism interface. We supply that as I mentioned earlier via a large multi-stakeholder regime.

So, there are tools out there. Could they be stronger? I think that's a great question.

GIANFORTE: Thanks. My time is expired.

SCHAKOWSKY: Now I'm happy to yield to Congresswoman Matsui.

MATSUI: Thank you very much, Madam Chair, and I want to thank

the panel for being here today. This has been a very enlightening discussion. And I just want to make a comment about the elephant in the room although I don't really regard it that way.

As you can tell, I'm from California. And there's been a lot of comment about the California law. But may I just say about California? There has not been much action on the federal front. We all know that and California being California with this myriad of businesses both big and small and its diversity, we have rural areas, urban areas and suburban areas. And it's not something that we're not a small state. We have a myriad of opinions and we also are a very innovative state, the home of many of the large companies that actually testified last spring.

So, I just will tell you this. There are ways that I know Mr. Grimaldi is saying he's already working with the State of California. I think that's really very important. But I must say also that it is something to be considered that it's a state that has -- is large enough to really be able to enact a law, but also to bring in many of the stakeholders, too. So, that's my piece on California.

I want to talk about advertising. Advertising supported models generate revenue through user provided data. Many platforms have broad statements that claim "What's yours is yours. You own your content." I appreciate that. But I want to understand more about that. To me, that makes users ought to have some say about if, how, and when it is used. But online platforms having an evolving set of rules for how partners can interact with user content and how the platform may modify or adapt this content as it is distributed.

And hearings of this committee has helped demonstrate that the real crux of the issue is how content is used and modified to develop assumptions and influences about users to better target ads to the individual. I want to ask. How should a federal privacy law ensure consumers have a meaningful say about how their data is used even when that data has modified use to develop inferences supplemented by additional data or otherwise?

And I'll start with you, Ms. O'Connor.

O'CONNOR: Thank you so much for that question. We would believe

that there should be limitations on secondary use of data that you provided for a particular service, and obviously transparency around the operations of the company and their intended use.

I think your question gets the heart of the matter, which is that individuals do not want to be discriminated online or offline and they want to know how the decisions that are being made about them are affecting their daily lives. So, we would absolutely want to look at issues of discrimination again in the online/offline world based on the data that is collected and allow the individual greater agency and control over that data.

MATSUI: Thank you. Now, it's been noted that advertising is

less concerned with identifying the individual per se, than with the activity of the users to predict and for consumer behavior, but I wonder if that's becoming a distinction without a difference. Even when user content isn't associated with that user's name, precise information can and is gathered through metadata associated with messages or tweets.

For instance, online platform often offer geospatial metadata that they provide by parsing messages for locations, names of interests including nicknames. This metadata could then be associated with other publicly available social media data to re-identify individuals.

Ms. O'Connor or Mr. Grimaldi, so even though advertising itself may not be considered with identifying the individual in the context of federal privacy law, how do we ensure data is not being used by others to do so?

Mr. Grimaldi first?

GRIMALDI: Sure. Thank you, Ms. Matsui. And I think that those

are very important questions that a potential new strong oversight regime would contemplate. A number of folks have mentioned the Federal Trade Commission.

They have brought 500 cases or more on issues around these types, and while they are incredibly capable and very strong, they don't have the resources right now I think that would allow them to play a role in a massive part of the American economy. So, I think that that is up for discussion as to whether or not a new paradigm, the one that we're contemplating could bring new oversight and new enforcement, and that's part of what we're discussing now.

A moment ago, I think it was Mr. Soto or Mr. Cardenas mentioned the jurisprudence in the past around these issues and I think it would -- I was a staff from this committee when long after the 1996 Act was passed and there was much discussion about why that was never updated, why were there was never momentum behind that to update it.

And I think it's because getting in the way of innovation and getting in the way of consumers enjoying what they want and the services they provided is a sticky thing. But in terms of more

oversight and new powers to protect consumers, I think we're at a place right now where we need to seriously think about that and make it happen.

MATSUI: Okay. Thank you. I've run out of time. I yield back.

SCHAKOWSKY: And next also from California, Congressman

McNerney.

MCNERNEY: There's a lot of us from California. Thank you.

Thank you. I want to thank the witnesses for your perspectives on this. It's an important subject and it's complicated. It's not something you can get your hands around easily. So, thank you very much.

My first question goes to all the witnesses and please just answer yes or no. Is it important that any law that we draft be able to adapt to technological innovation and advancements over time, starting with Ms. Collins.

COLLINS-DEXTER: Yes.

(UNKNOWN): Yes.

(UNKNOWN): Absolutely yes.

GRIMALDI: Yes.

(UNKNOWN): Yes.

MCNERNEY: Unanimous. Well, that makes my point. In order for

comprehensive privacy laws created by this slow-moving Congress to meet the current challenges and to be able to adapt to new circumstances, I believe it's critical that we give the FTC APA rulemaking authority for privacy and data security. I've called for this over time and I expect to see that in our policy.

My next question will go to Ms. Collins-Dexter. When Facebook's CEO testified before this committee, I asked him if I could download all of my data that Facebook had and he said unqualified yes. And then, later in the hearing after being advised by his staff that that wasn't correct, he corrected his statement. Now, Ms. Collins-Dexter, if the CEO of a major company that deals in data, that's their business, isn't sure what data they make available to its users, can we have any confidence at all that these companies will actually make their data available to users when requested?

COLLINS-DEXTER: No, we can't.

MCNERNEY: Well, good, and clearly it's important that the

comprehensive data privacy legislation grant consumers the right to access their data and to correct it if it's wrong. You're not raising your hand to make a statement.

COLLINS-DEXTER: No, I agree.

MCNERNEY: Thank you. Again, Ms. Collins-Dexter, can you explain

the risks that location tracking poses for low income Americans like so many of constituents?

COLLINS-DEXTER: Yes. And also, if I may, I want to sort of take

a step back again. I think there's been like a lot of conversation around patchwork legislation. And while I think that there are certainly issues with GDPR, there's improvements to be made with California legislation, I think one thing that I think came up in the testimony with Mark Zuckerberg that I think which you identify is really part of the shortcomings here is really an issue around tech monopolies and how they're consolidating power.

And so, I really think that it's important for us to maintain that as we're looking at the ways in which they're collecting innocuous data points such as geo-location in order to ascertain things around race, income and use that as an opportunity to use in predatory payday lending advertising, junk food marketing, and all sorts of sort of harmful advertising targeted at communities in different locations.

MCNERNEY: Thanks for that comment.

Well, I think it's important that we limit the use of data location information and that's something that I'm working with members across the aisle on. Again, Ms. Collins-Dexter, in your written testimony, you mentioned that algorithms work as kind of a black box to drive exclusionary practices and you need to raise -- you need to ensure that fairness in automated decisions. What do you think are some of the challenges that companies face in this today?

COLLINS-DEXTER: Yes. I think part of what we're looking at or

thinking about is this proposition of kind of "garbage in, garbage out", right? And so, I think there's a lot of presumptions that algorithms can't be biased or that tech is neutral. And what we find as history -- a long history of systemic inequities are actually being inputted from our data points and then replicating models of discrimination free from accountability.

And so, I think one of the things that we want to look at is kind of the algorithm distribution of advertisements related explicitly to education, employment, and housing opportunities, algorithmic distribution of political advertisements and communications and algorithmic determinations of product prices and same-day shipping. These are examples of some of the things in which I think we need to see more intelligence and information on.

MCNERNEY: Thank you.

I mean, Ms. O'Connor, I'm worried about data security as well as data privacy. Would you agree with that?

O'CONNOR: Yes, sir.

MCNERNEY: What's the relationship between privacy and security?

O'CONNOR: They are inexplicably linked. They are two sides of

the same coin. In our draft proposal, we copy some of Congressman Schakowsky's language about threshold and best practices and it is an essential part of a privacy program for any company, large or small.

MCNERNEY: Thank you.

And I just want to say I was shocked by your earlier statement, Ms. Collins-Dexter, that discriminatory technology is lucrative to identify ethnicity. In other words, it's a lucrative technology used nefariously.

Thank you. I yield back.

SCHAKOWSKY: And now, Mr. O'Halleran, for five minutes, you're

recognized.

O'HALLERAN: Thank you, Madam Chair, and I thank, too, the

witnesses also that appear before us today.

I'm all for national policy, but it has balanced. It has to be balanced for the good of the people of America and their privacy. We have to recognize that there's -- not only are these changing times, but the speed at which technology is changing has to be taken into account.

I was a former investigator and I have to tell you, I would love to be an investigator in these times because of the speed of information that I can get that used to take me maybe a month to get, I could get in minutes maybe. So, we have to be very concerned about these issues.

And this is a national dialogue on how to enhance the data privacy of consumers. It's a debate that is important not only to the people of my district in Arizona but the American people. I have to kind of thank California and I thank Europe for getting us pushed. Do I agree with necessarily what they want to do? No. But, do I think it has allowed us to be pushed in the right direction in a timely fashion? Yes. We should have done this much sooner. As members of this committee across the aisle, we must take seriously our duty to closely examine how to ensure consumer privacy remains protected in today's increasingly connected global economy.

Mrs. Zheng, as you know, my rural district in Arizona is home to many small businesses who constantly strive to compete in a modernizing economy and Internet ecosystem. Under current law, the Federal Trade Commission serves as the primary enforcer for Internet privacy as prescribed by the FTC Act. Taking into consideration the FTC's mandate to combat unfair and disruptive trade practices against consumers, what privacy framework do you see as striking the right balance between protecting the rights of consumers and helping ensure regulatory certainty for small businesses?

ZHENG: Thank you for that question, Congressman. I would note

that in a number of laws as well as legislative proposals, lawmakers have contemplated an exception for smaller, medium-sized businesses. I assume that that is something that this body will also contemplate.

The Business Roundtable, we do represent large American companies, but many of our companies do business with small companies as their clients or as their suppliers. So, we certainly care about the well-being of the small business community. I think there are different types of thresholds you could look to in considering possible small business exception including potentially the number of

records held or the annual revenue. But I'm not certain that the Business Roundtable is really the best organization to pontificate on what specifically that threshold ought to be.

O'HALLERAN: The reason for my question is because I want to see

that there's a protection for businesses across the entire spectrum, not just for those with large business concerns.

Ms. O'Connor, in your testimony, you state that existing privacy regimes rely too heavily on the concept of notice and consent. (Inaudible) place an untenable burden on consumers. As we all know, consumers often overlook the extremely dense language, here I am, in your user agreements and simply accept in order to get Internet applications and services.

Under any new consumer privacy statute, how could privacy notices be simplified for consumers whether they're technologically experts or novices, to better and more meaningfully understand how their information is being stored, used and if applicable, shared after accepting privacy agreements. And I will say that I believe the chairwoman was correct in her stack. It's probably a much bigger stack and we have to design something that works for the American people. Please.

O'CONNOR: Thank you, sir. That's exactly right. The number of

hours and the number of words we would all have to read on a daily, or weekly, or monthly basis to stay up to date on the choices we're making online and about how our data flows are staggering and overwhelming to any busy consumer.

I think there should be things that are inbound again for the furtherance of the transactions, the primary purpose of the deal. There should be things that are simply out of bounce like taking biometrics for purposes that are far field from the primary purpose of the transaction and then you could limit notices to that middle ground of things that are less clear that consumers might want that are related to the transactions that they have or their relationship with the company.

They definitely need to be shorter, clearer, and more to the point, but notices alone do not get us where we need to go.

O'HALLERAN: Thank you. And I yield. Thank you, Madam Chair.

SCHAKOWSKY: And now, I'm happy to yield to my colleague from

Illinois, Mr. Rush.

RUSH: Thank you, Madam Chair. And I want to thank all the

witnesses who have a hearing before the subcommittee today.

I (inaudible) subcommittee in 2007. I introduced a data bill back in 2007 and we're sitting here today discussing data, data security, and a data bill. And I hope that the current chairman (inaudible) and that we'll pass in Congress and the president we will sign. And so, I look forward to it and I've been pretty impatient about it.

I read the news by (inaudible) data files (inaudible) H.R. 1282 and one information (inaudible) in this section of data (inaudible). And I just wanted to know am I on base, Ms. Collins, trying to rein in (inaudible) consumers' data.

COLLINS-DEXTER: Yes. I think that's your right to be concerned.

There's like so much work we have to do. I think one of the things that I try to articulate in my comments that I think is super important is that 50 years ago as a country, we made a sort of social, legislative, and legal contract that said that certain things would no longer be accepted in our society.

People being turned away from lunch counters was not acceptable, people hanging signs that said "No Jews or dogs allowed" were no longer acceptable. And we didn't throw our hands up at that time and say, "Don't go to that restaurant," right? We took an ethical and moral stance and not just that, it was about knowing that if we could compete globally and thrive economically, we would ensure that we had more taxpaying members of our community, more people able to have opportunity and be economically mobile.

And so, part of (inaudible) with this like privacy legislation is basically looking at stopping (inaudible) online. It's around simply looking at our online (inaudible) and ensuring that those same laws that we created 50 years ago to prevent discrimination apply to laws online.

RUSH: Ms. O'Connor, what should we do to regulate data brokers?

O'CONNOR: Thank you, sir. And I think underpinning so many of

the questions today is the issue of opaque or surreptitious surveillance or data collection and that's the position -- again, and I just want to (inaudible) with Ms. Collins-Dexter because she is so right

that the of fairness of transparency, of accountability, and of equality for all Americans, data brokers really came up because of the Fair Housing Act, Equal Opportunity Act, and of providing fair credit to all Americans. They served at a time a purpose.

Right now, the opaque and surreptitious behind the scenes data collection by third parties that Americans do not understand or do not know about is fundamentally untenable going forward. So -- and I think the CEO of one of those companies is actually directly across the hall right now. So, maybe we could go ask him some of these questions, but they do have a purpose and to the previous comments, we need to reform. We need transparency. We need greater control and accountability over these third parties.

RUSH: In your testimony you discuss how (inaudible) draft

legislation and I quote you, (inaudible) to formulate rules (inaudible) advertising present particularly in those that result in unlawfulness and violation of civil rights law (inaudible). What should these rules look like?

O'CONNOR: There are good laws on the books as we all know about

discrimination and what that looks like in the offline world. However, intimate and real-time decisions can be made about us in the online world prior to knowing who we are based on inferences, on patterns of surfing and habits.

We would simply want to make sure that each individual's world view is not proscribed and limited by judgments that are made about them by companies that they are not aware of, that they are -- a child in one part of the country is not seeing ads for educational opportunities or a grown up is not seeing credit opportunities that that person is being served based on judgments companies are making about them without their knowledge.

RUSH: Thank you, Madam Chair. I yield back.

SCHAKOWSKY: Now, it is my pleasure last but not least to call

on Representative Kelly also from Illinois.

KELLY: Madam Chair, Illinois is holding it down for you -- or

with you. Thank you, Madam Chair, for holding this hearing today. As we've heard repeated news stories about breaches and data collection malpractice it's time for federal privacy legislation.

As the founder of the Tech Accountability Caucus, I want to follow up on the discussion of use of limitation. Ms. O'Connor, in your testimony, you described two buckets of use limitations, the first of which you referred to is unfair data practices. The CDT draft legislation prohibits secondary uses of certain sets of data like biometric information and health information. Can you clarify something for me? Other than the specific exceptions listed, is it your intention in the draft that these seven unfair categories are just not permitted?

O'CONNOR: That is correct, ma'am, that the secondary use of

those categories of data would not be permitted. Each individual would have to enter into a separate contract or agreement for a separate device.

KELLY: I know we've talked about doing this hearing about

(inaudible) and all of that, but a company cannot even see opt-in consent for their users. Is that correct?

O'CONNOR: It is an entirely separate transaction. That's right.

KELLY: Okay. How did you decide the types of data that

necessitated the extra protections?

O'CONNOR: The Center for Democracy and Technology worked over

the last several years, we have stood for and been in favor of omnibus privacy legislation for the entire 25 years of CDT. But we have reenergized to date internally and worked with academics across this country and around the world, business partners, other advocates in society, and looked at the research and the consumer research in this area and that's where we ended up with the list that we created.

KELLY: Okay. Thank you.

And to the panel, are there certain types of data that shouldn't be used at all, we can just run down from, Ms. Collins-Dexter?

COLLINS-DEXTER: Yes. I think there's certain pieces of like

personal identifiable, geo-location, things like that that I think should not be collected and kept.

KELLY: Dr. Layton, just your opinion to any data that shouldn't

be used at all or collected.

LAYTON: Thank you, Congresswoman, for that question. I think

that the question deserves a little bit of nuance. What we're talking about here is that that deserves an opt-in consent standard and I think the answer to that is likely yes.

For example, geo-location data, they actually -- the current guidance right now is that you acquire opt-in consent for geo-location data. What the Business Roundtable proposal recognizes is that there are sensitive categories of data that do absolutely needs protections, obligations including potentially opt-in consent.

KELLY: Thank you.

GRIMALDI: I would chime in by saying in order for the online

ecosystem to work, there would be data to render (inaudible) to provide services. So, in addition to -- of the prohibited pieces that we've heard today that we all agree on, how do we expand that list to include other things in the marketplace, that as my (inaudible) also mentioned (inaudible) getting such blowback or just on their face, too personal, too off limits to be used by other companies.

I think that's important and we need to make sure that the value that consumers are getting from their online experience can still be reaped even as we expand that list and we would love to work with you on that.

ZHENG: Congresswoman, I just want to -- I didn't want to take a

position on this because I know of important health and academic studies that under today's circumstances in the GDPR that data cannot be collected, but data that had been collected in the past has been used today to make very important conclusions for health questions.

So, I only urge -- I just want to put a note of caution. I understand that we have these concerns, but don't necessarily picture how the data may be available. So, I would tend to fall on the side of identify -- where we can identify that it's sensitive and have a higher standard, but not necessarily to outlaw it altogether. I'm just concerned about the future because I've seen these studies that going forward we won't be able to do these important health outcome studies in the EU.

KELLY: Thank you.

Anything else for the good of the order? I will yield back the balance of my time. Thank you.

SCHAKOWSKY: So, in closing, first, let me request unanimous

consent to enter the following documents into the record: one, public citizen framework from Privacy and Digital Rights for all; two, a letter from the Americans for Prosperity; three, a letter from Computer and Communications Industry Association; four, a letter from the ACLU and 42 other civil rights organizations; five, a letter from Main Street Association; six, a letter from Consumer Technology Association; seven, Engine Consumer Privacy Comments; eight, letter from Engine; nine, letter from American Bankers Association; 10, the NRF letter; 11, NRF comments; 12, Electronic Transactions Association letter; 13, 21st Century Privacy Coalition letter; 14, ACA International letter; 15, Representative Escher's opening statement for the record.

You can see the kind of broad spread interests. I want to thank our ranking member, the staff that works so hard on all of this. Thank you, and especially our witnesses for your participation today in this very first hearing of the session dealing with this issue of data privacy which is clearly going to go forward. I encourage you to also keep in touch as we move forward. We welcome your input.

I remind members that pursuant to committee rules, they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared. I ask each witness to respond promptly to any such request that you may receive.

(UNKNOWN): Wait, there's more.

SCHAKOWSKY: There's more.

Okay. So, we'll have a letter from the American Action Forum to put in the record; a letter from the Council for Citizens Against Government Waste; letter from Consumer Tech -- I see, letter from the Coalition for Secure, Transparent Internet; letter from R Street Institute; a letter from United Chamber of Commerce; a letter from Digital Liberty; a letter from the Internet Association; DOJ Cyber Digital Task Force; a letter from Google. Is that it? There's more.

Okay. You're right, a lot of interest. Okay. So, I have the public citizen -- I think the public citizen framework Privacy and Digital Rights For All; the Electronic Transaction Association letter; the letter from the National Association of Mutual Insurance Companies; a letter from Information Technology and Innovation Foundation; and along with the others, I ask unanimous consent to put these in the record, so ordered.

And now, I think at this time, the subcommittee is adjourned.

END

Feb 27, 2019 11:30 ET .EOF

-0- Feb/27/2019 16:30 GMT