Feb 28 2019 17:22:11
TRANSCRIPT

February 27, 2019

COMMITTEE HEARING

SEN. ROGER WICKER, R-MISS.

WASHINGTON, DC

SENATE COMMERCE, SCIENCE AND TRANSPORTATION COMMITTEE HEARING ON POLICY PRINCIPLES FOR A **FEDERAL DATA PRIVACY FRAMEWORK** IN THE UNITED

STATES

Bloomberg Government

Support: 1-877-498-3587

www.bgov.com

SENATE COMMERCE, SCIENCE AND TRANSPORTATION COMMITTEE HEARING

ON POLICY PRINCIPLES FOR A **FEDERAL DATA PRIVACY FRAMEWORK** IN

THE UNITED STATES

FEBRUARY 27, 2019

SPEAKERS:

SEN. ROGER WICKER, R-MISS., CHAIRMAN

SEN. JOHN THUNE, R-S.D.

SEN. ROY BLUNT, R-MO.

SEN. TED CRUZ, R-TEXAS

SEN. DEB FISCHER, R-NEB.

SEN. RON JOHNSON, R-WIS.

SEN. CORY GARDNER, R-COLO.

SEN. JERRY MORAN, R-KAN.

SEN. DAN SULLIVAN, R-ALASKA

SEN. SHELLEY MOORE CAPITO, R-W.VA.

SEN. MIKE LEE, R-UTAH

SEN. TODD YOUNG, R-IND.

SEN. MARSHA BLACKBURN, R-TENN.

SEN. RICK SCOTT, R-FLA.

SEN. MARIA CANTWELL, D-WASH., RANKING MEMBER

SEN. AMY KLOBUCHAR, D-MINN.

SEN. RICHARD BLUMENTHAL, D-CONN.

SEN. BRIAN SCHATZ, D-HAWAII

SEN. EDWARD J. MARKEY, D-MASS.

SEN. GARY PETERS, D-MICH.

SEN. TOM UDALL, D-N.M.

SEN. TAMMY BALDWIN, D-WIS.

SEN. TAMMY DUCKWORTH, D-ILL.

SEN. JON TESTER, D-MONT.

SEN. KYRSTEN SINEMA, D-ARIZ.

SEN. JACKY ROSEN, D-NEV.

WITNESSES:

MICHAEL BECKERMAN, PRESIDENT AND CEO OF INTERNET ASSOCIATION

BRIAN DODGE, COO OF THE RETAIL INDUSTRY LEADERS ASSOCIATION

VICTORIA ESPINEL, PRESIDENT AND CEO OF BSA - THE SOFTWARE

ALLIANCE

JOHN LEIBOWITZ, CO-CHAIRMAN OF THE 21ST CENTURY PRIVACY

COALITION

RANDALL ROTHENBERG, CEO OF THE INTERACTIVE ADVERTISING BUREAU

AND WOODY HARTZOG, PROFESSOR OF LAW AND COMPUTER SCIENCE AT

NORTHEASTERN UNIVERSITY SCHOOL OF LAW, TESTIFY

WICKER: This hearing will come to order. Good morning to you

all. Today, we held our first hearing -- this Congress -- to discuss policy principles for a Federal **Consumer Data Privacy** Framework.

I'm glad to convene this hearing with my good friend, Ranking Member Cantwell. We live during an exciting time of rapid innovation and technological change. Internet-connected devices and services are virtually everywhere, in our homes, cars, grocery stores and right here in our pockets.

The increase in Internet-connected devices and services means that more consumer data than ever before is flowing through the economy. The economic and societal benefits generated by the consumer data are undeniable.

From this data, meaningful insights are gleaned about the needs, preferences and demands of consumers and businesses alike. These insights spur innovation, help target investment and create opportunities.

The material benefits of data include increased productivity and efficiency, reduce cost, greater efficiency, greater convenience, and access to customized goods and services that enhance our safety, security and overall quality of life.

While the benefits of consumer data are immense, so too, are the risks. Consumer data in the digital economy has become a target for cyber criminals and actors that exploit data for nefarious purposes. This problem is exacerbated by the failure of some companies to protect consumer data from misuse and unwanted collection and processing.

These issues threaten to undermine consumers, trust in the Internet marketplace, diminishing consumer engagement in the online ecosystem. Consumer trust in the Internet marketplace is essential. It is a driving force and the ingenuity and success of American technological advancement, and prosperity.

Congress needs to develop a uniquely American data privacy framework that provides consumers with more transparency, choice and control over their data. This must be done in a manner that provides for continued investment in innovation, and with the flexibility for US businesses to compete domestically and abroad.

It is clear that we need a strong national privacy law that provides baseline data protections, applies equally to business entities of online and offline, and is enforced by the nation's top privacy enforcement authority, the Federal Trade Commission.

It is important to note that a national framework does not mean a weaker framework, and those that have already passed in the US and overseas, or being contemplated in the various states.

Instead, it means a pre-emptive framework that provides consumers with certainty that they will have the same set of robust data protections, no matter where they are in the United States.

We welcome our distinguished witness panel, Mr. Michael Beckerman, President and CEO of Internet Association; Mr. Brian Dodge, Chief Operating Officer of the Retail Industry Leaders Association; Ms. Victoria Espinel, President and CEO of BSA - The Software Alliance; Mr. John Leibowitz, co-chairman of the 21st Century Privacy Coalition; Mr. Randall Rothenberg, CEO, the Interactive Advertising Bureau, and Dr. Woody Hartzog, Professor of Law and Computer Science, Northeastern University School of Law and College of Computer Science.

I hope our witnesses will address the critical issues that this committee will need to consider in developing a Federal Data Privacy Law, including how best to protect consumers' personal data from being used in ways they did not consent to when collected by the stores or websites they visit.

How to ensure that consumers are presented with simplified notices about what information an organization collects about them, instead of lengthy and confusing privacy notices, or terms of use that are often written in legalese, and vary an organization's data collection activities.

How to enhance the FDC's authority and resources, in a reasonable way, to police privacy violations, and actually gets bad actors anywhere in the ecosystem. How to create a framework that promotes innovation and values the significant contributions of entrepreneurs, start-ups, and small businesseses to the U.S. economy.

How to provide consumers with certainty about their rights to their data, including the right to access, correct, delete and port their data, while maintaining the integrity of business operations, and avoiding unnecessary disruptions to the Internet marketplace.

And how to ensure a United States data privacy interoperable with international laws to reduce compliance burdens on U.S. companies with global operations.

I look forward to a thoughtful discussion on these issues, and I want to welcome all of our witnesses, and thank them for testifying this morning. And I will now turn to our Ranking Member, Senator Cantwell.

CANTWELL: Thank you Mr. Chairman, and thank you for holding

this important hearing. And welcome to the witnesses today, as we discuss moving forward on developing a Federal Data the Privacy Framework.

Last year, we learned that political consulting firm, Cambridge Analytica, gained unauthorized access to personal information of 87 million Facebook users, which it used for profiling purposes.

That same year, Uber announced that hackers had successfully gained access to the personal information of 57 million riders and drivers. The year before, in 2017, hackers successfully stole the personal information of 143 million consumers from Equifax, because the credit reporting giant failed to install a simple software patch.

And, just last week, UConn Health, announced that an unauthorized third-party accessed employee email accounts, potentially exposing personal and medical information of approximately 326,000 people.

These are not isolated incidents, or even one-offs. They are the only latest in a barrage of consumer privacy and security violations, many of which are entirely preventable. And consumers are at the receiving end of this reckless practice.

So I hope that Congress does grapple with Federal Privacy Data Legislation. What Congress has been successful in the past, in addressing certain types of personal information, such as health, or financial data, or children's information, consumers continue to see the challenges that they faced with corporate practices that allow for collection, storage, analyzing, and monetizing their personal information.

Back, just two years ago, Congress voted to overturn the FTC Privacy Rule that would have protected online users from Internet service provider, but had yet to take effect. So while we have gone backwards, in some ways, there are others who are moving forward.

In May of 2018, the European's General Data Privacy Regulations went into effect, providing the EU and its citizens with an array of new protections from certain types of corporate data practices.

And, in addition, the state of California has recently passed the California consumer Privacy Act, which also provided California citizens with new rights and protections, and this law goes into effect in 2020.

So, together the implementation of these two pieces of legislative policy, GDPR and CCPA, have brought new insight to the Congressional efforts to pass meaningful privacy and data security laws.

What is clear to me is, we cannot pass a weaker federal law just at the expense of States. So, Mr. chairman, I am certainly open to exploring the possibility of meaningful, comprehensive federal privacy legislation. I want to work with you and all the members of this committee, many of which have already introduced various pieces of privacy legislation, for thoughtful discussion about how we come to a resolution on these issues.

I don't think anyone should be under the illusion, though, that this is an easy task. The information age is still unfolding. The many challenges that we will face as new ways that information is shared cannot just simply be decided today. There are hard issues about how this economy will evolve. But I know that we can have a thoughtful exploration of the multi-faceted issues regarding federal policy that go beyond the stalemate that we have had for several years.

If we are going to deliver meaningful privacy and security protection for the deserving American public, then we must think about what this paradigm really looks like in this debate. I believe that just noticing consent are longer no longer enough. I don't think that transparency is the only solution.

So at today's hearing, I hope we kick off a very substantive discussion to explore how we go about changing this mindset that treats personal information as such a commodity for profit and think about it, as we have in tackling a series of hearings here, mr. chairman, on the various issues related to consumer privacy and security.

I know that there are members of both sides of the aisle who are very committed to this cause, and I hope we can make progress on this. Thank you, Mr. Chairman.

WICKER: Thank you very much Senator Cantwell. We now welcome

our distinguished witnesses. And we'll just start, at this end of the table, with Mr. Leibowitz. We ask each witness to limit opening remarks to five minutes. Mr. Leibowitz, thank you, sir.

LEIBOWITZ: Thank you so much, Mr. Chairman and Ranking Member

Cantwell. Other members of the committee, appreciate your inviting me to testify today, on behalf of the 21st Century Privacy Coalition.

To begin, let me state unequivocally, the Coalition, which is composed of the nation's leading telecommunications companies, supports strong federal privacy legislation that gives consumers more control over their data. It's the right thing to do for all Americans.

And we want to commend this committee, and particularly Chairman Wicker and Senators Blumenthal, Moran and Schatz for the thoughtful bipartisan work you have done to move that process along.

Simply put, Americans deserve meaningful privacy protections that give them the right to decide how their personal information is used and shared. The passage of privacy laws in Sacramento and Brussels has demonstrated that elected officials can enact privacy protections.

Now, you can demonstrate that same commitment for Americans, but you can do it better. Mr. Chairman, to get privacy right, we believe the best place to start is the landmark 2012 FTC Privacy Report, which I brought with me today.

During my time at the agency, we thought a lot about the best statutory design for protecting privacy and, after more than two years, based on decades of privacy enforcement, we produced a framework, praised by privacy advocates for its muscular approach to protecting privacy.

And the principles embodied in that report remain the centerpiece of the FTC's privacy regime today. Here's what that report called for. Greater consumer control over data, more transparency, privacy by design, oft-in rights for sensitive information, opt-out rights for non-sensitive information, rights of access and deletion, where appropriate, and a comprehensive technology neutral framework.

And these are all ideas, by the way, that we're also supported by the Obama Administration. Why? Because privacy shouldn't be about who collects consumer data, it should be about what data is collected, and how its protected.

Strong protections should be backed up by strong enforcement authority for the FTC, America's top privacy cop. Congress should provide my former agency with the ability to impose civil penalties for violators for first defenses, so malefactors don't get a second bite at the consumer deception apple, as well as additional resources to support its mission. And perhaps, some APA rulemaking that could be with guardrails.

We also recognize that the states have an important role to play in protecting privacy, which is why attorneys general should have the authority to enforce any new federal privacy law.

In addition to being the right thing to do, Mr. Chairman, enacting federal privacy legislation is necessary in light of the patchwork of privacy bills being produced in legislatures around the country. That's because what makes the Internet magical is also what makes it a poor subject for state legislation. It connects individuals across state lines.

Imagine if there were 50 different FAA standards, one for every state, the inevitable confusion could cause disastrous consequences in the air. Well, the confusion caused when consumers try to navigate through 50 states cyber cyberspace standards could cause digital disasters as well, and, at the very least, consumer confusion.

What's more, in their rush to address the need for stronger privacy protections, state lawmakers are drafting, and sometimes passing, legislation in haste. California's law puts tough tech neutral limits on the sale of information and heightened restrictions on children's information.

But the law also suffers from multiple drafting flaws, for example, it defines personal information based on households, when we all know that different people, living under the same roof, can have very different privacy preferences. And notably, California state lawmakers pre-empted their own municipal privacy legislations -- regulations.

A Bill being considered in Washington state is promising, but also not problem-free. Indeed, Mr. Chairman there are currently 94 privacy proposals pending in state capitals, 94, involving various and differing regulatory schemes.

The unintended consequences of these efforts don't just fall on large corporations, they hit small businesses, they stifle innovation, they balkanize commerce. Mr. Chairman, as you know, pre-emption in its best form is taking the most successful aspects of state policies and making them part of a regime that benefits everyone.

For these reasons, the 21st Century Privacy Coalition, has a view that you should pass strong, national privacy law -- a strong national privacy law, based on the FTC framework, that gives consumers more control over their data, provides greater transparency, and allows enforcers to sanction any digital gangsters who abuse the public trust. Thank you.

WICKER: And thank you very much, Mr. Leibowitz.

Mr. Beckerman, with the Internet Association, you're recognized for five minutes, sir.

BECKERMAN: Thank you, sir. Chairman Wicker, Ranking Member

Cantwell, members of the committee, thank you for inviting me to testify today. My name is Michael Beckerman. I'm the President and CEO of the Internet Association, which represents over 45 global Internet companies.

Our members include enterprise and consumer facing businesses that vary in size and business model. I ask that my full written testimony and Internet Association's detailed privacy principles be submitted for the record.

WICKER: Without objection.

BECKERMAN: The internet creates unprecedented benefits for

society and I'm here today to discuss why enacting state-of-the-art privacy legislation that protects all Americans, in a meaningful way, across industries, across technologies, from coast to coast, both on and offline, is in the best interest of consumers.

People want and expect more, and we will deliver. Let me be crystal clear, enacting a nationwide, modernized U.S. privacy framework that provides people meaningful control over their data, across all industries, on and offline, is the top priority for our members, and is imperative for the future of our economy and society.

We support getting this kind of legislation to the president's desk and sign into law this year. The Internet industry, and our member companies, are far from perfect. We fail and succeed based on people's trust, and we need to do better. We don't always get it right. We've made mistakes, we own up to them and we're using these challenges as an opportunity to improve.

That commitment to improve is driven by the top executives at all of our companies and supported by employees, engineers and the entire teams. We can always do better, and if you look at the transparency, and tools that exist online today, you can see that commitment, and the improvements that we're making on a daily basis to do better for customers.

The Internet is the greatest engine for individual freedom, and empowerment, and growth that the world has ever known. Our member companies are the embodiment of the American dream, a free enterprise and optimism about what is possible, and we want to get this right. And we're committed to improving trust and transparency. And just as important, we want to work with every member of this committee to get world-class privacy legislation done.

A globally respected American regulatory framework must prioritize protecting individuals' personal information, and foster trust through meaningful transparency, control, accountability and enforcement. People should have access and control of their data, and be able to move, correct, and delete personal information, but the burden should not solely lie on individuals.

Many foreign governments come through the American innovation hubs that we have across the country in every state to better understand the magic behind our industry in order to replicate it in their countries. Today, seven of the top 10 Internet companies in the world were founded here in the United States. That's something that's worth protecting, enabling, and being proud of.

The Internet is one of our great American exports. Internet Association also has traveled around the country and visited states, many of your states as well, and we heard directly from small business owners and community leaders who use data and Internet platforms to grow their business, communicate with customers, and bring the community closer together, and hire new employees.

These are the real winners of a data-driven community. It's important to note that non-tech, small businesses in every state, city, town and community, across the country, have the most to lose, if we get this legislation wrong, or if we end up with a patchwork of state laws.

Data has revolutionized every part of our economy in our daily life. It allows easy access to stay in touch with loved ones, from a distance, to get to work on time, with efficient navigation, to find the perfect playlist based on curated recommendations, and build communities around shared interests.

Data also enables companies to find you better products, show you more relevant content, and get you answers you need quicker, but even with the positive benefits, people have the right to know who is using their data and how. There should be no surprises.

This needs to hold true not only for the companies that have a direct relationship with customers, but also on and offline, but also for the thousands of businesses, that maybe you've never even heard of, that have and use your data without your knowledge.

Specifics that we're supporting here, in my written testimony, but speaking very broadly as I wrap up, this law should create one uniform standard that gives individuals control, makes companies accountable, and includes meaningful enforcement. People should have access to the data they share, be able to move, correct, and delete it when it's not necessary for a service.

And there should never be a surprise about who has your data, or how it's being used. In closing, the Internet industry is one of the most customer-centric industries in the world, and while we're already taking tangible steps to provide privacy tools, and protections for people in the U.S., and around the world, we're also committed to working with members of this committee, and other stakeholders to get meaningful privacy legislation signed into law. Thank you.

WICKER: Thank you, Mr Beckerman, and let me commend both of our

first two witnesses on impeccable timing on the five-minute rule. Mr. Dodge, you are now recognized.

DODGE: Thank you, sir. Chairman Wicker. Ranking Member

Cantwell, members of the committee, My name is Brian Dodge, and I'm the Chief Operating Officer for the Retail Industry Leaders Association. Thank you for the opportunity to testify today about consumer privacy, federal data privacy legislation, and the care that retailers take in approaching privacy.

Despite the rapid transformation of the retail ecosystem, our members' core business remains straightforward. To sell products and services to customers. To do so, retailers have always sought to know their customers well in order to serve them better. All methods and technologies may have changed. Leading retailers are guided by this simple purpose, and it is why we care so deeply about the conversation we're engaging in today.

Retailers support Congress's leadership in finding a sensible path to set clear privacy expectations for all Americans through federal data privacy legislation. The convergence of retail and technology has transformed the retail industry and greatly empowered consumers.

Today, while consumers can still reach retailers and physical stores, they can now connect through websites apps and through search and social media platforms. Competition to retail is now a click, or a voice command away. This competitive environment means that retailers must maintain and deepen the trust in customer relationships.

Robust competition ensures a daily referendum in the state of a retailer's relationship with their customers. Unlike some tack or telecom companies who tend to dominate their sectors, if a customer loses trust in one retailer, they can easily shop with another. These critical customer relationships shape retailers approach to meeting consumer privacy expectations.

As retailers look to personalize the shopping experience, they rely on data that customers provide and data that they collect when customers interact with their brands. Retailers who better know their customers can offer products that customers want. Whether it's stocking Ole Miss shirts and blankets in football season, or the Red Gonzaga gear in basketball season, personal information helps retailers decide how much merchandise to buy. where it needs to be, and when.

Customer data not only helps retailers make important decisions throughout their supply chains, but it also produces dividends for customers. For many retailers, loyalty programs are an essential component of their business model and one that provides mutual benefit. Customer data also enables the services customers demand. For busy families, the ability to pick up groceries with the convenience of drive-through is a game-changer.

Customer data also enables beneficial curated experiences. Offerings like baby registries enable new parents to discover curated products that they might not know they will need. Personal information fuels other services leading retailers provide to benefit communities, such as flu trackers. These flu trackers are compiled using retail prescription data across thousands of stores.

Leading retailers recognize a unique moment that we are in today. There's bipartisan opportunity to create a uniquely American privacy framework. RILA believes that a federal privacy framework should be designed to protect customers and provide clear rules of the road for individuals, businesses and for the government. Retailers are prepared to accept the responsibility of new privacy requirements to create a national framework that inspires consumer confidence.

Retailers are prepared to accept the responsibility of new privacy requirements to create a national framework that inspires consumer confidence. RILA believes that there are six critical elements to a pragmatic, workable approach to privacy at scale.

One, customer should have control access, correction and deletion rights of their personal information. Two, a sound policy framework must pre-empt state laws to set clear expectations for all consumers and reduce state-level burdens on interstate commerce. Three, accountability for every sector within the data ecosystem is essential for a risk-based approach to privacy is necessary. Critical to this approach is a precise and targeted definition of personal information. Five, a federal policy should create incentives like safe harbors for good-faith actors to go beyond baseline privacy requirements. And, finally, six, retailers support fair, consistent and equitable enforcement of privacy laws through an empowered Federal Trade Commission and State Attorneys General.

In closing, retailers are committed to working with Congress to develop a strong federal privacy standard based on these elements to protect consumers without stifling innovation, investment and competition. Thank you for the opportunity to testify today, and I look forward to your questions.

WICKER: Thank you, Mr. Dodge, and thank the ranking member. And

I want to thank you for the references to Ole Mis sand Gonzaga. And also, if you just wanted to do one reference that would have touched both of us, that would have been Mississippi and Gardner Minshew, who have made his way to Washington State University and was an outstanding quarterback.

Just getting that little plug in there. Miss Espinel, we're glad to have you.

ESPINEL: Thank you. Good morning Chairman Wicker, Ranking

Member Cantwell, and members of the committee. My name is Victoria Espinel, and I'm the president and CEO of BSA - The Software Alliance. I commend the committee for holding this hearing on the important topic of a **federal data privacy framework**, and I thank you for the opportunity to testify on behalf of BSA.

We are here today, because the Americans people's trust has been broken. Every morning, people wake up to a news report about their location being sold without their knowledge. When they go online, their movements around the web are tracked allowing companies to profile them. Companies that people have never heard of often know more about them than they know about themselves. And companies buy and sell that information to the highest bidder.

Sometimes the information is used for a legitimate purpose, but sometimes it is not, and this is unacceptable. BSA is the global advocate for the software industry. BSA members have business models that promote, not undermine privacy and security. Our businesses are not dependent on selling ads. There are different business models and different approaches to consumer data. There are different incentives when a company's business model is primarily the monetization of personal information.

The driving force behind the success of our companies is the sale of innovative products and services, such as cloud computing, design and engineering, cybersecurity protection. Our customers pay for these products and services. We are partners with businesses of all sizes across every industry in the US economy, helping them grow and thrive. But we know that we are not the only actors in the ecosystem and we agree that it's time to clean it up.

We want to ensure that companies use data in a way that empowers not exploits. We call on Congress to pass strong, comprehensive privacy legislation based on three pillars, rights, obligations, and enforcement. First, legislation should give consumers the right to know and the right to control what happens to their personal information. Second, legislation should require strong obligations for companies to safeguard data and prevent its misuse. And third, legislation should provide strong, consistent enforcement.

Let me begin with consumer rights. First, consumers should have the right to know the categories of information and organization collects, how that information is used, and how it is shared. Again with consumer rights, first, consumers should have the right to know the categories of information. An organization collects how that information is used and how it is shared.

Second, consumers should be able to use that knowledge to exercise real control over their personal information, to say no to data being used in ways that they don't want. Certain data, for example, health data, or financial data, or information about a particular health condition a person

might have is particularly sensitive, and companies using that data should first obtain explicit consent.

Third, people should be able to access correct, delete and obtain a copy of their data. There may be important limits on these rights, for instance, protect network security and free speech, but those limitations should be the exception.

The second pillar is strong obligations for companies. Consumer rights should be reinforced by obligations on companies to handle data responsibly. Companies that handle personal data should have mechanisms to ensure safeguards against privacy risks, including security breaches, and inappropriate use of consumers data.

Congress should also ensure that a federal privacy law provide clarity about the responsibilities of companies that play different roles in the complex data ecosystem. All companies should have strong obligations, but those obligations should fit the kind of business that they are in, and distinguish between controller and processor.

The third pillar is enforcement. A strong federal law also needs strong enforcement. The FTC should continue to be the primary federal enforcer, but it needs new tools and the resources necessary to carry out its mission effectively. The FTC should have new authority to issue fines to hold companies accountable.

Today, the FCC cannot issue a fine the first time a company violates Section 5, no matter how egregious. That is wrong and it should be fixed, and we believe that State Attorneys Generals should be able to enforce a strong, comprehensive federal privacy law on behalf of the residents in their states.

In closing, let me emphasize, a federal law does not and should not mean a weak law. A strong federal law to replace state laws without undermining privacy protection. States, such as California, have been leaders on this issue. Passing laws aimed at enhancing privacy protections.

The objective of a consistent national standard is not to weaken privacy protections provided by California or other state laws. Rather, our aim is to strengthen privacy protection by providing comprehensive, clear and consistent protection for consumers across the country.

The privacy framework I've outlined would help rebuild consumers trust. Now is the time for Congress to act. BSA stands ready to assist in the effort to accomplish this important goal, and I look forward to your questions.

WICKER: Thank you very, very much. Now Mr. Randall Rothenberg

with the Interactive Advertising Bureau.

ROTHENBERG: Chairman Wicker, Ranking Member Cantwell, members

of the committee. I am honored for the opportunity to testify today. I'm Randall Rothenberg, Chief Executive Officer of the Interactive Advertising Bureau. We represent more than 650 leading media and technology companies, consumer brands, and there are hundreds of thousands of employees.

The IAB develops technical standards and best practices to create efficient, effective and safe digital marketing environments. We train industry professionals on these standards and practices, and we field critical research on the role of interactive marketing, and growing brands, companies and economies. Our experience shows there is a ready path forward to assure both the safety of consumers and continued growth in the consumer economy.

The Internet is the most powerful and empowering mode of communication and commerce ever invented. It is built on the exchange of data between individuals, browsers, and devices, and myriad server computers, operated by hundreds of millions of businesses, educational institutions, governments, NGOs, and other individuals around the world.

Advertising has served an essential role in the growth and sustainability of this digital ecosystem almost from the moment the first Internet browsers were released to the public in the 1990s. In the decades since, data driven advertising has powered the growth of e-commerce, the digital news industry, digital entertainment, and a burgeoning consumer brand revolution.

But the source of the Internet's innovation is also the source of its vulnerabilities. The data exchanges that fuel new businesses and drive unprecedented cultural invention can also be used to violate consumer security and privacy. The question before Congress is, how do we close off the sources of corruption without impeding the innovation? It's no easy task. The economy is in the midst of an enormous shift. Data increasingly is the core asset of every enterprise, replacing such legacy assets as a company's manufacturing footprint, or its access to raw materials.

The greatest consumer brands of the 20th century are now being challenged by thousands of upstart brands in every category, which share one trait, whether they make luggage, or beer, or cosmetics, or eyeglasses, or underwear, their success is premised on having individual relationships with millions of consumers. This is achieved only through the responsible use of data.

IAB strongly believes that legislative and regulatory mechanisms can be deployed in ways that will reinforce responsible use of data and enhance trust in the Internet ecosystem, while avoiding the

unintended consequences that can result from ill-considered regulatory regimes, notably in the erection of barriers to market entry, and reinforce advantage for the largest incumbents.

IAB has the ability to help guide Congress, based on our experience building effective mechanisms to protect consumer privacy and security. These include the digital advertising alliances, your ad choices, and political ads programs, which provide consumer with transparency, control and accountability in their digital advertising experience.

Our industry is heartened by the federal government joining us in our long-standing effort to put enhance privacy and security. Our model is the partnership between government and industry that created the modern concept of automotive safety in the 1960s. Yes, that partnership began as a shotgun wedding. Yes, the auto industry resisted at first, but an undeniable consumer right to be safe on the highways met well-researched solutions, which the Congress embedded in well-crafted laws that were supported by the states.

The result has been millions of lives and billions of dollars saved. The analogy holds well here. Americans have a right to be secure on the information superhighway. Our goal should be to find the five or 10 practices and mechanisms, the seatbelts and airbags of the Internet era that companies can implement and consumers can easily adopt that will reinforce privacy, security and trust.

To begin, we believe it is vital that government, industry and consumer organizations establish a new paradigm for data privacy in the United States. In developing this new paradigm, IAB cautions to Congress from relying on legal regimes, such as Europe's General Data Privacy Regulation, or California's Consumer Privacy Act as models. These pose stringent mechanical requirements on businesses, but fall short in giving consumers real rights and choices.

Opt-ins and opt-outs, I would suggest to you, are not the seatbelts and airbags of the information superhighway. IAB asks for Congress support in developing this new paradigm. That would follow four basic principles. First, in contrast to many existing privacy regimes, a new law should impose clear prohibitions on a range of specifically identified, harmful and unreasonable data collection, and use practices.

Second, a new paradigm should distinguish between data practices that pose a threat to consumers and those that do not. Third, it should incentivize strong and enforceable compliance programs and thus universalize compliance by creating rigorous, safe harbor processes in the law.

And, finally, it should reduce consumer and business confusion by pre-empting the growing patchwork of state privacy laws. As with the rest of the witnesses, IAB asks for Congress's support in developing such a framework to enhance consumer privacy, and we want to work with you. Thank you for the time today, and I welcome your questions.

WICKER: And thank you, Mr. Rothenberg. Dr. Woodrow Hartzog, Dr.

Hartzog, I understand you have a Mississippi connection.

DR. HARTZOG: That's correct Senator. I am born and raised in Mississippi.

WICKER: And there was a TV personality named Woodie Assaf.

DR. HARTZOG: That's correct. It was my grandfather.

WICKER: Ah, terrific, good. Well, welcome.

DR. HARTZOG: Thank you. Chairman Wicker, Ranking Member Cantwell, and members of the committee, thank you for inviting me. Before I provide testimony, my name is Woodrow Hartzog, and I am a Professor of Law and Computer Science at Northeastern University.

My comments today, will address what I've learned from my research on privacy law. Specifically, I will focus on one particular conclusion. Our current privacy regime has too much of people and too little of those entrusted with our data. I make two recommendations for the committee.

First, I recommend that lawmakers should resist the notice and choice approach to data protection. It passes the risk of online interaction from data collectors on to people under an illusion of protection. The problem with notice and choice models is that they create incentives for companies to hide the risks of their data practices through manipulative design, vague abstractions, verbose terms, as they shift risk by engineering a system where we never stop clicking the "I Agree" button.

The transparency and control contemplated by these frameworks is impossible in mediated environments. People can only click on the options that are provided to them, and companies have incentive to leverage the design of their products to manipulate and wheedle people into oversharing.

Internet users are gifted with a dizzying array of switches, delete buttons, and privacy settings, but these choices are too often an overwhelming obligation. People might remember to adjust their privacy settings on Facebook, but what about Instagram, Twitter, Google, Amazon, Netflix, Snapchat, Siri, Cortana Fitbit, Candy Crush, their smart TV, the robot vacuum cleaner, their Wi-Fi connected car, and their child's Hello Barbie?

The problem with thinking about privacy as control is that, if we are given our wish for more privacy, it means we are given so much control that we choke on it. Meaningful data privacy reform must do

more than merely strengthen commitments to transparency, consent and control.

Second helpings of "I Agree" buttons, intrepid (ph) unreadable Terms of Use would not have prevented the Cambridge Analytica debacle, or the epidemic of data breaches, nor will they prevent the problems of manipulation, discrimination, and oppressive surveillance that we face in the future of automation. We are only just beginning to see the human and societal cost of massive data processing and platform dominance.

In addition to core privacy related harms associated with data collection and use, companies demand for personal information is negatively affecting our attention, how we spend our time, how we become informed citizens, and how we relate to each other. Phenomena like fake news, deep fakes, non-consensual pornography, online harassment, biased algorithms, over sharing on social media, addiction by design, and life spent staring into our phones, are at least partially attributable to, or made worse by the personal data industrial complex.

Marginalized communities, particularly communities of color, shoulder a disproportionate risk of privacy abuses. We need broader frameworks for personal data, not just because information is personal to us, but because the incentive to exploit it creeps into nearly every aspect of our technologically-mediated lives. My second recommendation is to adopt substantive and robust rules that protect people's trust in companies and establish firm data boundaries that companies are not allowed to cross.

Being trustworthy in the digital age means companies must be discreet, with our data, honest about the risk of data practices, protective of our personal information, and above all, loyal to us, the data subjects. Our privacy framework should be built to encourage and ensure this kind of trustworthy conducts.

Apart from rules, some practices might be so dangerous that they should be taken off the table entirely. A meaningful data privacy framework should also embrace substantive data boundaries for the design of technologies and rules limiting, or prohibiting data collection and use. And in cases where technologies represent a grave danger to our civil liberties, they should not rule out an outright moratorium or ban.

Finally, without structural supports, resources, and a strong political mandate for enforcement, any data protection framework will be ineffective. Regulators need rulemaking provisions were necessary, robust civil penalty authority, and the ability to seek injunctions. Individuals should have private causes of action and rights as data subjects. In order to protect hard-fought state privacy protections, federal legislation should continue the tradition of acting as a floor, not a ceiling for privacy rules.

In conclusion, our rule should seek to protect people and groups instead of saddling them with the risk of online interaction. Only then can our digital ecosystem become sustainable.

WICKER: Thank you, Dr. Hartzog, and thank you to all of our

excellent panelists. Let's start then with pre-emption. We know that the GDPR enacted by the European Union went from something that was advisory to the various member states of the EU to something that became a regulation. So there was pre-emption in the EU. We learned from Mr. Leibowitz that actually there was a patchwork of local privacy provisions in California and that state statute pre-empted the local. So, let me ask, let me start with you, Mr. Leibowitz. Why is this important? And particularly, with regard to our concern about consumers. Why is federal pre-emption, something that you advocate?

LEIBOWITZ: Well, you always want to take the perspective of

consumers, and I think Professor Hartzog made that point quite clearly. You don't want a cacophony, or a crazy quilt patchwork of 50 different state laws. It will make consumers numb to notifications. If someone is driving from Biloxi, Mississippi to Bellevue, Washington, they don't want to go from state to state, and have different regimes. And those regimes may be conflicting, and so where --

WICKER: I wonder if anybody's ever taken that drive?

LEIBOWITZ: I am sure, man. You know, I dropped a bunch of

state-to-state references, because I wanted to be under the five-minute rule, because I was told what would happen to me if I went over. So I'm sure people have taken that drive, and at least metaphorically.

And, I really, and it strikes us and our coalition, but really anyone, and most importantly, I think, most people on the panel, that you need to have one strong federal privacy regime. It needs to be strong, it needs to empower consumers, but if you do that, then I think the right approach is to pre-empt state laws, and make sure everyone is protected. And wherever you go, you are protected under that same tough rule.

WICKER: Dr. Hartzog, if we allow the federal law that we hope

to enact on a bipartisan basis here to be a floor, doesn't that leave us with the patchwork? And

where's Mr. Leibowitz wrong on that.

DR. HARTZOG: Senator, it does leave us with the patchwork, but that's what we've been dealing with for quite some time, and I think that while consistency is nice, I think that the patchwork actually, has been not something that has been insurmountable, in so much as, I teach my students to do with 50 state patchworks all the time. As a matter of fact we can actually pretty good at dealing with that.

And so, I think that's to the extent that we're dealing with 50 state patchworks as a problem. I don't see that as being insurmountable, because it's what we've been dealing with all along when dealing with data breaches.

WICKER: If you had been helping the E.U., would you would you

have left it as it was with differences among the member states of the EU?

DR. HARTZOG: Well, I think that's a difficult distinction to draw, simply because we're dealing with two entirely different systems and cultures. In the United States, we have a tradition of dealing with a patchwork of 50 state laws, something that that we've really been working with a while.

And so -- well, I think there are virtues to consistency. It's in my opinion, it's not the obstacle -- what strikes me as the first thing that we have to surmount if we're going to get privacy right.

WICKER: Thank you. Miss Espinel, about this distinction between

controllers and processors. Can you explain exactly what you meant there? What's the difference, and exactly what are you advocating?

ESPINEL: Thank you. I'd be happy to. So, first to be clear. BSA

companies act as both controllers and processors, and we believe that controllers and processors should both have obligations. We think the obligation should fit the role that they're in. So just to explain those terms a little bit. When a company's acting as a controller they are controlling the data, that is to say they are making decisions about how that data will be used, and we believe in that role they should have primary responsibility.

When a company is acting as the processor of data, they are merely processing the data. They should still have obligations, but again they should fit that role. So, for example, if they're processing the day that they should have an obligation to make sure the data is kept secure, because that falls within the role that they are in at that moment. I will add that one of the concerns that we have is that if exactly the same types of obligations are put on companies in both roles, you know as controller and as processor, we could actually end up undermining privacy protection.

And the reason for that is because, if you're acting as a processor, you don't necessarily have access, or visibility into that data. If the same types of consumer rights and obligations on companies are put in there, you would put a processor in the position of having to go and get access to personal information that they wouldn't necessarily have.

So we think it's both important to make the law effective and workable, but we often think it's important, because I think it could undermine privacy protection if we don't make that distinction.

Thank you. Senator Cantwell.

CANTWELL: Thank you, Mr. Chairman. I am -- I wanted -- I wasn't

really going to go with the pre-emption thing, but I just want to be clear since the Chairman brought it up. I mean, are we here just because we don't like the California law, and we just want a federal preemption law to shut it down? Or, do people think you can have meaningful federal privacy legislation without that? Just say yes or no from the witnesses.

(UNKNOWN): No.

CANTWELL: Thank you.

(UNKNOWN): I think Congress can do better.

CANTWELL: Mr. Dodge.

DODGE: We've advocated for a federal policy for some time,

prior to California, so we continue to do so.

CANTWELL: So you don't need pre-emption.

DODGE: We want federal pre-emption.

CANTWELL: Yes or no.

DODGE: Yes.

CANTWELL: OK. We think there should be a stronger federal law,

but you have to have pre-emption of states.

ESPINEL: We think that again -- we think we can do better. We

think California doesn't go as far as a federal privacy laws could go, and we don't want the privacy protection of a person to be dependent on the state in which they live. So we think a federal law would be better, And in doing that, should replace state laws that that are not as clear, and consistent, and as strong as you would hope a federal privacy law would be.

ROTHENBERG: Yes, emphatically with an asterisk.

(UNKNOWN): I don't think cream is necessary, and I think it

could be actively harmful.

CANTWELL: Thank you. Dr. Hartzog, I'm a little more in your

camp at this moment. I find this effort somewhat disturbing that, with all the litany of things and privacy violations I just went through, and as countries are grappling with, is the first thing that people organize here in DC is a pre-emption effort. What we need to do is get at the task you just outlined and Miss Espinel, you did a pretty good job too of outlining what are the challenges that we face.

Let's get on the same page, because I think us together getting on the same page about what are the consumer issues at stake here, and how do we want to protect them, I think we'll get us a better result than just this focus -- first of all, I don't see my California colleagues acquiescing to the Congress on this issue anyway. So I think what we need to do is be very, very clear here what are our challenges.

Miss Espinel, you mentioned fines and I'm curious as to what do you think, culturally, that sets the right message. We were very involved in setting standards on anti-manipulation after the Enron scandal. That is both at the FTC, CFTC and the FERC. And it was amazing to me how many companies thought they literally could be the owners of home heating oil and keep it off the coast just to drive up the price.

And, you know - so, I mean, literally people said, "Oh yeah, that's within our rights." Do you think we need a very bright line here that just creates the culture within various, you know, develop -- you know, online developments that will help make a culture within companies aware that these are the risks and threats?

ESPINEL: Well, I think I think we need to have a culture where,

when companies are handling consumers data, are using in various ways, what they are really focused on is the consumer. They are focused on the reasonable expectations of those consumers and very focused that have a -- on that. And so, I think -- I mean, I think that will be a cultural shift, at least for some companies.

CANTWELL: Well, you advocated an FTC fine, and my point is when

you have this general counsel at your firm warning people that there will be a fine for doing these kinds of things, that's a pretty bright line. Dr. Hertzog, do you have an opinion about this?

DR. HERTZOG: So I think that when we're thinking about these questions, it's importance, the pre-emption conversation seems to lump a lot of different things together, all at once, and it's worth sort of pulling them out. Not only are we talking about pre-emption as a way of consolidating possible enforcement efforts, or maybe not, but there's also the question of the cost of dispersed compliance.

And also, and I think that one of the reasons that I'm really skeptical of pre-emption is that we're, sort of, operating under this assumption that we figured out exactly what all the rules should be.

CANTWELL: I'm referring more to Miss Espinel's now point about

giving FTC clearer, fining authority. Is that a clear, easier, bright line to establish that would be helpful?

DR. HERTZOG: Oh absolutely.

CANTWELL: OK.

ESPINEL: In the first instance, and that I think often goes to

change the culture. Right now, in the first instance of a violation of Section 5, the FTC does not have finding authority. I think it will change cultures internally if companies know that for a first initial violation, the FTC has authority that Congress would need to give them to be able to issue a fine against that conduct.

DR. HERTZOG: And if I may add a point going back to your pre-emption question, Senator Cantwell, let -- we would encourage, and it's your panel's decision, of course, but we would encourage state AG enforcement. That's the approach on COPPA, which pre-empts. It gives state AGs the ability to enforce the statute.

CANTWELL: Thank you. Thank you, Mr. chairman.

WICKER: Thank you. Mr. Rothenberg, could you explain your

asterisk in 30 seconds?

ROTHENBERG: Certainly. clearly, you want consistency over

chaos. That's the argument in favor of pre-emption, but equally clearly there is a absolute role for the states to play in enforcement. And again, automotive safety is one of the many areas where you have federal and state enforcement and regulations complementing each other, along with industry self-regulation.

The trio is where you get the strongest opportunity to protect people's safety and privacy and security.

WICKER: Thank you, very much. Senator Fischer.

FISCHER: Thank you, Mr. Chairman. Miss Espinel, as Congress

looks to strengthen the data privacy, it's crucial that we prevent irresponsible data use to begin with, or on the front end, I think. As we look to define personal data, how it should be processed, and how a user might control their own personal data, what do you believe constitutes an unreasonable data use?

ESPINEL: Well, I think a use of data that goes beyond the

reasonable expectation of the consumer is inappropriate. And I think that is, you know, there are some of those uses that could be worse than others, but I think that's really what we need to focus on. We need to focus on, what is the reasonable expectation of that consumer? And ensuring that companies are only using data in ways that lines up with that reasonable expectation.

Another way of saying that, is that, you know, companies should be limited to uses that are relevant to the stated purpose of why they are using the data. So I think it comes back to the consumer, and having that as kind of the central tenant of how companies are thinking about their data. Having that trusted relationship, I think, with your customer, with the consumer, it's going to help motivate companies to do that.

FISCHER: OK. I would ask each member of the panel, if you can

give me one example of unreasonable data usage. Whoever likes to start.

LEIBOWITZ: Sure, when I was at the FCC, we brought multiple

cases involving -- dozens of cases, actually, involving companies that made a commitment that we will keep your data private. And then, they didn't. That's deception. And then we brought a number of cases that involve companies has just had inadequate data security. That was such that they didn't protect consumer data.

But we didn't have fining authority, you know, at the outset. I would say, which is something that our organization, 21st Century Privacy Coalition, supports.

(UNKNOWN): Thank you. I'd say if, if that is being used in a

way that a person would be surprised about that use, in a way that is unexpected to them, in a way that does not benefit the consumer.

(UNKNOWN): Building off that the relationship between retailers

and their customers is about buying goods and services. So anything that dramatically departs from that, in that context, would be a violation of the trust that's so important to retailers and their customers.

ESPINEL: So I'll give a concrete example to illustrate consumer

expectation. I think, when you put your location into a map service, it is your reasonable expectation that the map is going to use your location in order to give you directions.

I think, if you have a flashlight app that is tracking your location information, that is not something that a consumer, in my opinion, would reasonably expect, and so I think that would be an example of an inappropriate use in those circumstances.

(UNKNOWN): There are lots of examples we invent. Here's one.

I'm surfing the web, or on an app where I'm looking up recipes involving eggs and somehow that's going to insurance companies in order to deny me insurance, or to raise the price of my insurance, because it might have an impact on my cholesterol.

(UNKNOWN): An example that I would use would be the collection

of things like biometrics that were used for maybe authentication devices that within repurpose for things like surveillance across a wide variety of contexts.

FISCHER: OK. Good examples. A core component of the GDPR is to

guard against unreasonable uses of data through clear, explicit consent. And, however, in this case, we already are seeing an interface redesigns that undermine user choice and the opt-out functions.

We have numerous consent boxes that pop up online, or in applications, often with a threat that service cannot go forward, can't be used, unless the users going to consent to it. Besides being really irritating, they've had have that happen, I think we're left with an illusion of having some kind of control as users. Mr. Hartzog, do claims of complete user control, incentivize users to share more personal data?

DR. HARTZOG: Sure, I think they do. Who doesn't want more control? It sounds empowering, and when you have it, you feel like OK, well now I want to interact here. But I think the problem with thinking about privacy in terms of control is that treated as though the mere gift of it, it is a protection of privacy in and of itself.

When, actually, if we can't exercise that control, then it's meaningless and it's overwhelming, and it's a losery. And I think that that's why I don't think that control should be the only value that we might be placing here, even though it seems to be --

FISCHER: What do you want another value to be?

DR. HARTZOG: Sure. Well, there are several you could think of. One, would be trust relationships, right? So things that encourage trust between people. There are values of dignity. There are other values, control ostensibly serves autonomy, but it doesn't always sort of serve it. Obscurity, which is a value that we all sort of live in, that gets eroded over time that the control doesn't necessarily get at.

I think that that privacy, as a broad concept, can include lots of different values and it shouldn't be distilled down to just control.

FISCHER: Thank you. Thank you, Mr. chairman.

WICKER: Thank you. Senator Klobuchar.

KLOBUCHAR: Thank you. As you all know, I have a privacy

legislation with Senator Kennedy. Bipartisan legislation, and in part what I have found in getting involved in this, is that the reason all the states are doing all, this is that we have done nothing here. And part of it is, because the companies that you represent have been lobbying against legislation like this for years. And it's never right enough, or they've got your backs, and it happens time and time again.

I encountered this with the Honest Ads Act, which some of the companies now support, but there is a reason the states are doing this. So, let's not forget that when we talk about states and different patchworks of regulations.

So my first question is, one of the aspects of our Bill is that it requires 72-hour notice of a breach, and when I asked Mr. Zuckerberg about this when he appeared before the Committee, he said that such a requirement made sense to him. Are any of you against a requirement of some kind of notice that consumers be informed in a timely manner of a breach.

BECKERMAN: Consumers should, thank you Senator, consumers

should be notified in a timely manner. The challenge with having a very exact and prescriptive period of time, you could find situations where it could impede in an investigation --

KLOBUCHAR: OK. So just - I have so many questions. You're not

in favor of the 72 hours, Mr. Beckerman.

BECKERMAN: It shouldn't be exactly 72 hours, because that might

be impeding with an FBI investigation that could be plugging the hole, or going after the culprits, but they should be timely.

KLOBUCHAR: I'm sure we could find some exceptions for that. So,

Dr. Hartzog, in December, the "New York Times" revealed that Facebook gave certain tech companies like Netflix, Spotify, Microsoft, Amazon and others access to more user data, including private messages, without their explicit consent. Do you believe that companies are being fully transparent about sharing users data with third parties?

DR. HARTZOG: No, I think that, and the problem is, that there's a there's a trap here, which is you can either, sort of, be transparent with general abstractions in ways that are digestible and accessible, or you can, sort of, dump the entire volume of data practices on people, which would also not have the intended effect here.

KLOBUCHAR: OK.

DR. HARTZOG: Regulators might be.

KLOBUCHAR: Another issue is lengthy Terms of Service complex

language, which our Bill also gets to. Mr. Beckerman, last month, TechCrunch reported that two companies in your organization offered users, some as young as 13, either $20 cash, or gift cards to download research apps. And you believe these users actually understood the terms and gave true informed consent?

BECKERMAN: I think Terms of Service that exists both on and

offline need to be shorter and more simple, so people actually can understand. It doesn't make people more private or more secure, no matter what you're doing. If you need a law degree to read 320 pages, and so, we agree that they should be shortened down.

KLOBUCHAR: So you'd like to see that as part of federal

legislation to have plain language.

BECKERMAN: Absolutely. I mean, companies need to have these

short and concise. People can understand what they're looking at.

KLOBUCHAR: And how about opting out of having personal

information tracked and collected.

BECKERMAN: It's important that the tools that people have are

contextual, and so, you're able to not be surprised as you're using an app, or service on how information is being used, and the control goes with the individual. And, by the way, I just want to add, we support that.

KLOBUCHAR: OK, and also Mr. Leibowitz, our Bill actually

centralizes the authority to enforce the National Privacy Law with the FTC, and you believe that's the right thing to do?

LEIBOWITZ: I do in my current capacity, and I do in my previous

capacity. Yes.

KLOBUCHAR: OK, well that means you do.

LEIBOWITZ: I do twice.

KLOBUCHAR: OK, very good. The Honest Ads Act, I just want to go

to that. Mr. Rothenberg, I know you represent 650 leading media and tech companies. Some of the companies have endorsed this Bill. We now have 12, or 13 Republicans on the Bill in the House,

and we are working to replace Senator McCain, who we miss very much, so that we have some Republicans on this Bill in the Senate, given that all it does is require disclosure and disclaimers on political ads, just like you have on TV, and radio, and newspaper. So does your organization support the Honest Ads Act, and greater transparency in political advertising?

ROTHENBERG: Yes, Senator we do. We do have some reservations

with some pieces of it, because we think it potentially penalizes smaller publishers that are the -- in effect -- unwitting end nodes of the distribution of political advertising. Well, isn't strong enough in identifying the complexities in the supply chain for the distribution of political ads.

But by the same token, we, IAB, have developed a mechanism for transparency for political advertising. It's the only one in the marketplace right now --

KLOBUCHAR: But don't you think we should have rules of the road

in place? Otherwise some platforms will do different things --

ROTHENBERG: Absolutely.

KLOBUCHAR: -- the exact same patchwork that Mr. Leibowitz was

referring.

ROTHENBERG: Absolutely, we would love to have your legislation.

Look at our political ads disclosure mechanism that's currently in the market, and used as a safe harbor, or a model for the kind of --

KLOBUCHAR: Like I said, we have 12 Republicans on my Bill now

in the House, and so, the hope is, we will pass it there. And I hope we can pass it here, because 2020 is not far away. So thank you very much.

WICKER: Thank you, Senator Klobuchar. Senator Thune.

THUNE: Thank You, Mr Chairman, when I was chairman of this

committee, we held a series of privacy hearings to begin the conversation on what Congress should do to promote clearer privacy expectations, while ensuring that innovation and investments are not stifled. And so, I want to thank Chairman Wicker for making this a top priority of this committee, and I continue to look forward to working on this important issue.

And one of the key components to this debate is transparency. Transparency allows consumers to make informed decisions about the products and the services that they use. Many companies, some of which are members of the associations represented here today, note the transparency as a core value. However, the actions that they take raise serious questions.

Earlier this month, Google's nest home security devices were found to have a built-in microphone, which was not disclosed to consumers in any of the product material. Google stated that, and I quote, "The on device microphone was never intended to be a secret," end quote. However, even if Google's actions were not intended to mislead consumers, I do believe that there should have been better transparency with respect to these practices. Which is why I joined Chairman Wicker and Senator Moran this week in asking Google to clarify their practices.

Mr. Beckerman, the Internet Association released privacy principles at, among other things, call for transparency and controls over how the personal information that individuals provided companies is collected, used and shared. When developing a federal privacy framework. What should transparency policies look like to avoid the actions that Google and others have taken in the past?

BECKERMAN: Thank you Senator. And I agree in the case of the

microphone. Obviously, that's something that that should be disclosed and part of transparency is having people know what's happening. And whatever their expectations are, which vary by service, and your expectations vary by product, obviously, depending on what you're using, you should never be in a position where you're surprised. And companies need to make it clear what data is being used, and how it's being used, and what the benefit is to the individual. So that they are in control of that information.

THUNE: And how would you go about formalizing that? And, you

know, the privacy law?

BECKERMAN: Sure, part of that is to ensure that that companies

are accountable. A lot of the debate and what we're seeing, and one of the flaws actually with the California Bill, is that it puts way too much of the burden on individuals. Yes, it's important that people have control and companies give transparency, but as a number of the panels have noted, you can't just like throw everything at consumers and expect them to click through boxes and read all these documents to know. And so, if some of that is having accountability for the companies, and strong enforcement at the FTC to ensure that they're living up to that,

THUNE: Mr. Dodge, when Alastair Mactaggart, the California

privacy activist, testified before this committee last year, I asked him about concerns businesses have raised that the CCPA will prohibit certain practices consumers favor. Like, customer loyalty programs to reward their best customers. He indicated that the CCPA was not intended to hamper customer loyalty and rewards programs, and the concern, quote, "Mystified him." Could you elaborate on whether or not you find this to be a legitimate concern, and if it is, what changes would you like to see to the CCPA, or to federal legislation to address that concern?

DODGE: Thank you for the question, Senator. Our members do view

that as a concern, the lack of clarity around that, and other areas in the California law are problematic, as they anticipate compliance with the beginning of next year. I think, in terms of solving that problem, we're starting to do so today. And you did so last year, by starting a deliberative process here at the federal level to think through all of the different impacts of privacy legislation, and invite the perspectives of a wide array of audiences who care about this issue greatly, so that we can work through the various impacts, and avoid those kinds of challenges.

THUNE: And this, I just direct too quickly to all the

panelists. And that has to do with the question of whether or not you all support a technology neutral and sector neutral approach to federal privacy legislation. And that is to say, should Internet service providers, and edge (ph) providers, be subject to the same privacy requirements? Or, should federal legislation approach different business models differently? Whomever wants to take that from this panel.

ESPINEL: We think all companies should have strong obligations.

I think their responsibilities to fit the role, but we think all companies should have strong obligations.

THUNE: Does anybody disagree with that point of view?

(UNKNOWN): No, no. And I just want to add, we agree. And going

back to your earlier question, what can you do about the problems you raise? I think committee has the opportunity to move a national bipartisan bill that would allow opt-in and opt-out rights for sensitive data for consumers, opt-out rights for consumers, and strong enforcement at the FTC that would make sure that people don't do things that they know will cost them large amounts of money as they violate the law.

(UNKNOWN): Well, I happen to believe that this is one of the

areas, maybe not many areas in this next couple of years, that we ought to be able to come together around in a bipartisan way and come up with a national data privacy law that could be signed and enacted. And so, I hope that the discussions that we're having today will serve as a foundation for moving forward with legislation that that gets at this issue, because I think it's an important one to everybody in this country. It impacts literally everyone.

THUNE: So, thank you all for being here.

WICKER: Thank you, Senator Thune. Just quickly, Dr. Hartzog, do

you agree with Miss Espinel and Mr. Leibowitz on the tech neutral question.

DR. HARTZOG: So, I think that there are virtues of tech neutrality and in broad swaths. I think that it did advantageous, but I do see caution against a sort of ceaseless commitment towards technological neutrality and sector neutrality. Just because I think it could be dangerous to treat all industries as though they have the same incentives, and as though, they do operate the same way. And so, I've recognized those virtues, but would just push back against the total devotion to it.

WICKER: OK. Well, you might want to supplement your answer

there, and I appreciate -- Senator Schatz.

ESPINEL: And if I could on that, Mr. Chairman. Look, I do think

this is very instructive, particularly as it relates to what we did with HIPAA and Gramm-Leach-Bliley, and all these. You know, we've taken sectors, the financial sector. We've taken, you could even say, a little bit in the housing sector, but health care financial sector, and describe things by sectors on privacy issues, and in this legis. I'm not I'm not saying that's the end all and be all. I'm just saying, now we can look back at what we've done and how well did that serve us taking that kind of approach. Thank you.

WICKER: Thank you, Senator Schatz.

SCHATZ: Thank you, Mr. chairman. Thank you to all the

testifiers. I want to flesh out this question of transparency and control, because my judgment is, that it's fine. But in an IOT universe, and with lots of users being under 18, that it's just not practicable to expect that people are actually in control of all the dials that have to do with the Internet.

And when you're talking about billions of sensors, devices throughout your house, Dr. Hartzog give a few examples, but we're talking about by the time -- you know, 10 years from now, your toaster is going to be connected to the Internet. Your keys are going to be connected to the Internet. You're going to have theoretically, if we just did transparency and control, you can have hundreds of micro decisions every day that you're supposed to achieve informed consent about.

And that's setting us -- I mean, the practicability of that is a problem, but there's also this question of lots of kids use the internet and will automatically click "I Agree" not knowing what they're agreeing to. So, I'm not criticizing transparency and control as something we should not do, but I am saying it's insufficient. And that's why I think we have to talk more about what is the obligation of a company once they are in possession of your data.

First of all, there's tons of data already in the possession of companies, so we have to deal with that problem. Second of all, people are going to click "I Agree" irrespective of what the pros is, especially since everyone's going to be clicking "I Agree" on some kind of six-point font, while they're on the bus.

And so, Dr. Hartzog, I want you to flesh out this duty of loyalty. This idea that when you go into the doctor's office, they don't tell you to pick how that data is used. We're going to share it with the oncologist, but not the nurse's assistant. You just trust them. Then you go into your lawyer's office. It's not up to you to decide how that data is used. There is an affirmative obligation of the professional on the other side to not harm you. And so, I think any data privacy law has to have a backstop, not just turning the dials, but an affirmative obligation for anyone that is in possession of your data to not harm you. And Dr. Hartzog, I wonder if you might comment on that.

DR. HARTZOG: Absolutely. Thank you very much. I think that when we talk about trust, and we talk about this obligation of loyalty, and you could think about several different rules that we might envision, that would help enforce this. One of which would be a requirement in risk assessments, for example, to keep not just a very specific set of interests of the data subject in mind. But the data subjects entire well-being and not to elevate your own interests over the, sort of, generalized well-being.

And so, that can go in, you could talk about rules prohibiting abusive behavior that keep entities from leveraging people's own limitations, resource limitations, and cognitive limitations against them. So you can't use confusing language and triple negatives and interfaces designed to trick people, and extract and manufacture consent. In a corrosive way, and when we think about other sorts of obligations, obligations of honesty, that's more than just transparency. That's being forthcoming about things that that people want to know, that the companies might not prefer they know about.

SCHATZ: Right, but I just want to make the point, it's not just

about the disclosure. Yhey may disclose adequately.

DR. HARTZOG: Right.

SCHATZ: Even in plain language. Even in a way that a

13-year-old can understand. I'm not sure how that's doable, but that's -- even stipulate that that's possible. Still, there ought to be obligations not to harm customers. I want to get to the FTC really quickly. My judgment is that we ought to have some broad principles in statute and allow the expert agency to flesh that out over time.

And I think that includes rulemaking authority first, fine authority and additional staffing. And I know that's kind of a lot. But you guys are all conversant in all this. Is there anyone who disagrees with rulemaking authority, first fine authority, and additional staffing to enforce this overtime? I'll obviously start with our former FTC person.

(UNKNOWN): I strongly support additional resources. The size of

the FTC is the same now that it was in 1980.

SCHATZ: I have 40 seconds --

(UNKNOWN): OK, but strongly support more resources, strongly

support fining authority, want to see what the committee comes up with in terms of in terms of rulemaking, but some rulemaking with guardrails. I think we get support.

SCHATZ: I will accept a yes for anyone who wants to be --

(UNKNOWN): I definitely support more resources on the

rulemaking. There should be more direction from Congress on that and maybe a model similar to what we saw with COPPA would work.

(UNKNOWN): Support all three with the caveat of what we get to

the end of this process, we'll look at the legislation --

SCHATZ: Sure

(UNKNOWN): -- and when we can pass it.

ESPINEL: Yes, we support our role in rulemaking. Yes, we

support additional new authority for initial fining. And, yes, we support resources for the FTC, so they can do their job.

WICKER: I have grown up with the previous panelists and --

SCHATZ: Thank you.

(UNKNOWN): Yes, across the board.

SCHATZ: Thank you.

WICKER: Congratulations, Senator Schatz. Show of hands. No,

Senator Moran.

MORAN: Chairman, thank you. Thank you for you, and the ranking

member, having this hearing. Thanks for our panelists for being here. Let me pick up on where Senator Schatz concluded. I believe that, as we draft legislation that we need to provide clear and measurable requirements in statutory text for the FTC to utilize, while also including appropriate flexibility in narrow rulemaking authority.

And the goal there is, to put the broad words in place that Congress believes is appropriate. And then, to give the FTC authority to -- as technology changes, for example, to make decisions over time that narrow the scope. So I think what I heard from all of you is that there would be agreement in that regard.

You see value in having statutory requirements, and you see value in rulemaking authority by the FTC. And I heard a caveat, at least with one of you, which I think it makes sense to me. It does make sense to me that the guardrails are necessary in regard to that rulemaking authority. And anybody want to contradict what I think you all are agreeing to? Good.

Then, secondly, the question of fine, the ability to impose fines. So that makes sense to me as well. But let me have you explain for me how you think that civil authorities should work. One of the suggestions that the GAO made to enhance Internet privacy oversight with civil penalties for first-time violators. This is a report that GAO published last January. And again, I think I've heard all of you say that you'd be supportive of that kind of authority. Although I wouldn't be surprised, if some of you would want to tell me what that fine authority ought to be. Just broad fine authority? I want to narrow it down

(UNKNOWN): I'll just say it, you know, we want a high-level

standard, national standard. And we believe for it to be effective, it has to have teeth, which means giving the FTC the authority to define, in the first instance.

MORAN: And then Senator Schatz talked about the resources

necessary. I'm a member of the Appropriations Committee that funds the FTC. Maybe this is for you, Mr. Chairman - chairman, Leibowitz, when you say additional resources, what what does that mean? Senator Schatz said staffing -- what's missing at the FTC to do -- well maybe that the resources are inadequate today, but as we add greater authorities, what is required?

(UNKNOWN): Well, look. You don't want the quality of the

agency's work to be strained by the quantity of demands placed upon it. So that's at a high level. At a more granular level, the number of FTEs that the FTC is right about where it was in 1980, the population of the United States has grown by a hundred million since then.

We're talking about the most complex issues involving online data when you're doing investigations. And the budget has been flat since I was there in 2010, and so you need to give the Commission, I would say, more resources. I don't think you wanted like -- I don't think you want to say overnight double the size, because you can't do that. You want to grow it thoughtfully.

But I think, if you -- our belief collectively and unanimously at the Commission, was that if you could grow the Commission, a number of employees, by 10 percent a year over a period of time say five years, that would be -- that would be enormously helpful.

MORAN: Let me make certain that I also understand that it is

the FTC that we believe should have these authorities. Statutory authority should be granted the FTC, civil penalty aspects of the FTC. I think when we started this conversation, whatever that was years ago, over time it seems to me, that there's been a consensus growing about the FTC being the appropriate place to be -- to house the authorities we're talking about. Any disagreement from any of you in that regard?

ESPINEL: No, I would -- I we also believe the FTC should be the

primary enforcer of federal law, but we additionally would support having state attorneys General to have the ability to enforce on behalf of residents of their state.

MORAN: I think I misunderstood you. You said the FTC, not the

FCC.

ESPINEL: FTC.

MORAN: You said, FTC, correct?

(UNKNOWN): Yes. FTC. FTC. But we also support State Attorneys

General, and in COPPA, that's the regime that Congress gave to the FTC. The FTC enforces and state AG's enforce.

MORAN: OK. Thank you, Mr. Chairman

WICKER: And thank you Senator Moran. Senator Markey.

MARKEY: Thank you, Mr. chairman. Both Europe's and California's

new privacy laws acknowledge a fundamental principle that children and teens, vulnerable populations that deserve special, unique protections. Europe identifies children as vulnerable individuals who deserve specific protections. And under European rules that are already in place, there's a heightened measure for 13, 14, and 15-year-old.

While California's law establishes an opt-out standard for adults, it includes an opt-in standard for users under 16. These laws reflect emerging consensus that kids and teens are growing up in a world in which their personal information is a valuable commodity, so we must construct meaningful guardrails.

As the committee develops a comprehensive privacy bill, we should institute special safeguards for 13, 14, and 15-year-olds, who right now, have no protection under the law. Mr. Leibowitz, you agree that Congress has historically acknowledged on a bipartisan basis that kids are a vulnerable population deserving of special rules.

LEIBOWITZ: Yes, I do, and I think we see that in COPPA.

MARKEY: Yes. So I am the author of COPPA, the Child Online

Privacy Protection Act, the constitution for children's protection in our country. Miss Espinel, do you agree that COPPA is critical in protecting young people's privacy online?

ESPINEL: We do, and we thank you for your many years of

leadership.

MARKEY: So now, we have to update it. So, which is the standing

point, is up to -- its 120 and under in COPPA. Now, we have to go to the Facebook era now, that we live in, and 13 and 14 and 15-year-olds data being compromised. So Mr. Hartzog, do you agree that a comprehensive federal privacy bill should include special protections for children, 13, 14 and 15?

DR. HARTZOG: Yes, senator, I think that's the children particularly need to be able to be protected, and they need privacy to flourish. And notice and choice regimes fall particularly hard on them, because not only do children, sort of, lack the practice in making a lot of the decisions that we ask adults to make every day, but they lack a lot of the knowledge to make those decisions.

MARKEY: Should it be opt-in.

DR. HARTZOG: Yes, I believe so. I have no strong objection.

MARKEY: You agree with that Miss Espinel.

ESPINEL: I think our hope is that we end up with a federal

privacy legislation that is so strong that it will adequately --

MARKEY: But a minimum, but a minimum for kids we're talking, as

we do for adults.

ESPINEL: I think we think sensitive data for anyone should be

opt-in and we have a pretty broad --

MARKEY: I agree with you on that. I'm agreeing with you on

that. I'm just trying to carve out one --

ESPINEL: But in terms of distinction --

MARKEY: Yes

ESPINEL: -- between 13, 15, I will say that I completely

understand where you're coming from. I think we would like to have more conversations with you about that.

MARKEY: OK. Mr. Leibowitz, opt-in for 15 and under?

LEIBOWITZ: I would say at the very least opt-out for 13 and up,

and we want to work you on any legislation, you'd like to incorporate into the larger bill.

MARKEY: Thank you. Well, how about you, Mr. Rothenberg? Opt-in

for kids?

ROTHENBERG: The answer as Miss Espinel, and Mr. Leibowitz.

Obviously, as a principle, clearly. Devil's in the details. I worry about blanket prohibitions on all communications to 15-year-olds or 14.

MARKEY: It's not like a prohibition, it's just opt-in. Again,

we look at a California law and European law. OK, so if we pre-empt, and we make it lower than that --

ROTHENBERG: Yes. Again--

MARKEY: I think it will cause a big problem, if we lower the

standards.

ROTHENBERG: No. Again--

MARKEY: So I just put that out there as the reality of it, and

to make sure that we take kids and put them out of bounds, in terms of just having the extra special

protection. The bill also includes an eraser button for kids by requiring companies to permit users to eliminate publicly available personal information submitted by the child.

That's already again the law in California. Mr. Hartzog, you have written about the importance of allowing users to delete content that they posted as children from the Internet. Why is that so important, and should we build that protection into the law?

DR. HARTZOG: Sure, absolutely. I think it's because of the way in which we develop as humans, if the ability to, sort of, interact within these zones of privacy, and not have things that were created a while back, sort of, stay with us. That the ephemerality (ph) is an important protection, and we should embrace it.

MARKEY: Yes. And on the question of discriminatory use of

information when men and women differentiated other categories, do you think we need to take account of that and any law that we passed? So that we don't have that discriminatory contact online.

DR. HARTZOG: I will agree with that.

MARKEY: OK. I thank you, Mr. Chairman. Again, kids have to be

given an extra level of protection. They're vulnerable, they're targeted, and without building that in, I just think it makes no sense to me in California, or --

WICKER: Anybody want to disagree on the eraser button. No one.

OK. Senator Blackburn.

BLACKBURN: Thank you, Mr. Chairman. Thanks for calling the

hearing, and I have to tell you, it is like reliving old times to sit here and hear Ed Markey talk about these issues. We did this in the house for years as Mr. Leibowitz remembers well and I'm sure Mr. Beckerman too, it was in 2013. We started working on privacy and data security in the House, and trying to push toward a national standard for privacy, and push towards some data security provisions.

Of course, 2014 was a year of the breach. We realized that it needed to be done. So hopefully we can help the Senate now cross that. Miss Baldwin with us. She was there in the House, as we debated, they said energy and commerce. I do think that it is important that we get these right, and that we do it right and that we not give people a false sense of security. And that is the reason that I led the push to get rid of the FCC's 2016 Privacy Order, because I felt like that did give a false sense of security.

I also introduced, one of the first bipartisan, certainly the first in the House, bipartisan bill on privacy, the Browser Act. and Mr. Leibowitz would say, I loved your comments, you kind of went through all the provisions that are in that bill. And, as we work on a product here, I do hope that those standards are included. And that we do have Miss Espinel, coming back to your comment, one set of standards for the entire ecosystem, because that provides clarity, and it helps raise consumer awareness.

I want to talk for just a minute. Mr. Beckerman, I'm going to start with you, and I know you've seen all the articles that have been in the press lately about the app developers sharing sensitive data, sensitive information with Facebook and others. There was also the Cambridge Analytica issue. We now have the Nest issue, so many scandals.

And I think that you would agree, and probably all of you would agree, we now realize this data sharing is not a bug, it is a business, it is a business model, and big tech has made a whole lot of money by exploiting the use of this data. And it's one of the reasons that we have to come together. We're glad to hear you all say, you're going to come together and work with us on it, because as Miss Klobuchar said, you spend a lot of money fighting this, and that goes back to 2013, when we started on this.

So Br. Beckerman, your members, should we expect them to give consumers more or fewer privacy protections when they are downloading these apps? And we should expect more or less clarity from them in the data that they are choosing to share.

BECKERMAN: Thank you, Senator. And thanks for your leadership

on this issue for for many years. Consumers deserve more, and we want to make that very clear. We support this Bill and, as you've noted you know, this is an online and offline, all the apps, all the companies, everybody should be part of this, and people should get more.

BLACKBURN: OK. So then, what are you doing to encourage these

companies to be more transparent and to provide more protections? Because it's nice to come in

here, and talk about what we're going to do? You all have been doing this for years, but we're not seeing the action, and the protections that are embedded in these processes.

BECKERMAN: Absolutely, I mean, and while we do need a federal

approach that pre-empts the states as we talked about to get it right for both small businesses and individuals, our companies are taking steps every day, adding new tools and useability for people to delete their accounts, delete information, bring information between services. So all the things that we're talking about in our principles are things that are being rolled out.

BLACKBURN: OK. So every one of you, each of you, have talked

about trust and having trust with individuals that your virtual you is protected online. So, Mr. Beckerman, what are your people doing? And when you talk about trust as a priority, is it, or is it not, it's a top priority? Is it middle of the way? Do you just give it lip service? How are you approaching that?

BECKERMAN: Trust is number one. If people don't feel safe --

BLACKBURN: They don't trust you now. So what are you doing to

make -- ?

BECKERMAN: People still love and value the products and service

that our companies provide, and I know, there's a lot of bad cases that we can read in the newspaper all the time. But it's important to note all the positive uses for data, and all the positives that these companies and products bring, and people still do like it. However, it is incumbent on all of us to ensure that we maintain that trust, and not abuse it, and not take it for granted.

BLACKBURN: We look forward to some positive actions. I yield

back.

WICKER: Thank you, Senator Blackburn. Senator Blumenthal.

BLUMENTHAL: Thank you, Mr. Chairman. Let me begin by thanking

the chairman for having this meeting. Also senator Thune for his work before now, and thank both the Ranking Member, Senator Cantwell, and Senator Wicker for their leadership in this area. What you have heard here is profound distrust on both sides of the aisle with the situation that exists right now. In a sense that we've passed whatever the turning point is for Congress to act.

We have been working diligently, Senator Wicker and myself, Senator Schatz and Senator Moran on solutions here, and we enlist, and urge your participation. But simply to second what Senator Klobuchar said. You have to convince us that you really want something more than pre-emption. You have to convince us that your clients really want change in this area, because the overwhelming evidence so far is that they're willing to look the other way, to put profits ahead of people here.

And so, I think that we have a trust gap that we need to bridge, and most consumers simply have no idea about the vastness of their vulnerability, because they have no real comprehension about how much data is collected, whether it's their locations, through all kinds of mechanisms that exist to track them, or the voices of their children through toys that they use, or biometrics that are gathered in the name of security.

The depth and breadth of data collection is like a vast galaxy out there, unknown to most consumers. And I want to urge you to, in effect, put your money where your mouth is. I don't mean that disrespectfully in any way, but we all know that industries involved here have a record of looking the other way, or ignoring their obligations in the specifics, and that's involved the granular efforts that are required.

Let me begin by asking, how many of you believe that Americans deserve the same level of privacy now as a floor that California provides for its people? You can just raise your hand. How many of you feel that California ought to be a floor, not a feeling?

ESPINEL: We believe strong federal privacy legislation could go

beyond California and improve on California.

(UNKNOWN): Senators, correct me, to be perfectly clear, the

federal Bill needs to be worthy of pre-emption, and we're not talking about weakening California. What we're looking for is something actually that gives people more and better and more meaningful privacy than what California does.

And there's things in the California Bill that has been pointed out that actually make people less private, and we think this committee and Congress can do better. It makes me --

BLUMENTHAL: There should be a floor, not a ceiling. It should

be stronger than California.

(UNKNOWN): Stronger than California.

BLUMENTHAL: Do you agree, Mr. Leibowitz. We believe stronger

and better.

(UNKNOWN): We agree. We think it's very instructive in setting

federal stems.

BLUMENTHAL: Instructive

(UNKNOWN): Instructive as --

BLUMENTHAL: So it should be even tougher.

(UNKNOWN): We should be a high standard.

BLUMENTHAL: Well, I'm asking you.

(UNKNOWN): Yes, if --

BLUMENTHAL: You can say no, but I don't tell me it's

instructive. OK. What do you think, it's the minimum

(UNKNOWN): The absolute sentiment of the California law is to

give it strong control of users and transparency, which we fundamentally believe with. We could quibble with some things around the edges, but I do think it sets a very high standard, and would be a good floor for federal legislation.

(UNKNOWN): Absolutely and we can go further. We should start

with a set of rights, of human rights, that exist in this digital environment. We should bring those down to a set of principles that can be followed. Senator Schatz's legislation starts in this direction, and then we should talk about specific prohibitions, and specific allowances, and then about specific mechanisms that can further these rights and these principles.

(UNKNOWN): I would agree, though, I'd focus on the fact that

that pre-emption is not just about providing, sort of, better, more or less protection, but also about questions of nimbleness and ossification. And so, I think that that treating California as a floor is the start. But that's not the entirety of the pre-emption debate.

(UNKNOWN): What we really need is a privacy Bill of Rights that

is expansive and flexible, just like our constitutional Bill of Rights is.

BLUMENTHAL: Correct. Thank you all.

WICKER: Thank you, Senator Blumenthal, Senator Capito.

CAPITO: Thank You, Mr. Chairman, and thank all of you for being

here. We have had several hearings, and Mr. Chairman, I appreciate this one. There's a question, I've wondered, and I'll start with Mr. Beckerman just because I think that might be a natural start, but I'd like to hear from all of you. In our committee hearings, we've heard a lot of pushback on the GDPR, and then some confusion with the California law as well. You just now, all of you, advocated for better, and more stringent, is the way I heard it, more stringent privacy parameters than what's offered under the California law.

But in an international company, and I believe this to be true, even if we set a standard here, you still have to comply with the GDPR. Am I correct?

(UNKNOWN): Yes, senator.

CAPITO: Thank you. I mean, this is an important point too. It's

important that we have a system that's interoperable with GDPR, and that's one of the, I think, criticisms from many about GDPR is, that it's very, very expensive to comply with, and very complicated, where a lot of small and medium-sized businesses have decided that they're no longer able to do business in Europe because of this law.

(UNKNOWN): And I don't think, that's a model that we want to

take here, and it's another reason why, having one federal strong approach, that small and medium-sized businesses in every state can comply with in easy way without having to hire teams of lawyers to comply with, is a better approach.

CAPITO: Yes, so I guess my point is, if it's with the larger

companies that are still remaining to do business globally in the EU that, that you're already complying with that standard, complicated or not, you're going to have to keep complying with that standard complicated or not. So I don't know, maybe I am looking at this the wrong way, but I mean, I certainly don't know all the weeds of all the regulatory things in the GDPR.

But would it in the end, be simpler and easier for ease of business to have that standard be the standard for the companies that's already getting applied to, rather than have two separate standards?

(UNKNOWN): If I could take that Senator Capito. In some ways it

might be simpler, but it wouldn't be better. And so, as you're designing a framework. What you want to do is make sure that you have the benefits of stronger privacy protection, and there's a clear consensus on this panel that's what you want to do.

CAPITO: Right.

(UNKNOWN): And it's hipartisan, and that is great, but you also

don't want to undermine innovation. So, for example, there are some early reports that suggest that, that innovation has slowed down, new business models have slowed down, the "LA Times" pulled out, and so did Pottery Barn. Pulls out of Europe because they don't want to have to comply.

CAPITO: Right.

(UNKNOWN): So I think you want to run privacy protections. I

think, if you want more trust from companies, you need a front strong federal backstop. You don't want multiple clicks away, but then you want to design the legislation that's going to allow for innovation, while also protecting consumers.

CAPITO: Thank you, I would say, you know, I joined the course

of the bipartisan support for consumer privacy. I mean, my questions, I'm going to go then. How do we guard against in creating this new standard here in the United States? How do we guard against what we already see has happened in Europe and that's the smaller businesses that can no longer comply? How are we going to guard against that in terms of creating this business standard? What challenges does that bring as well? Seem to have a thought.

(UNKNOWN): Yes, Senator. As I've been saying, I think,

consistency built on rights, principles, and actual mechanisms will allow the clarity for smaller businesses to remain competitive. In your quest --

CAPITO: Without the high cost.

(UNKNOWN): Without the high cost. Your question to Mr.

Beckerman began with referencing larger companies.

CAPITO: Right.

(UNKNOWN): They do this, but that's the problem. Larger

companies will always have the resources to be able to invest in this.

CAPITO: Right.

(UNKNOWN): We just have to be cognizant. We have scores and

scores of newspapers that we know of that have pulled out of Europe, because of the cost of compliance with GDPR.

CAPITO: Right. I also appreciate the conversation on the

youthful children, and young teens being able to have some more protections, but you know at the other end of the age spectrum, there are issues as well. And I think, as we all age, we're going to be reliant on our Internet capabilities a lot more than say the generation who's 85 to 90 now.

And we know that scams around seniors are prolific in just about every household. I don't know how you think about it, but think about that when you're putting together your standards, because I think that could bring about, you know, it's -- I don't want to say a country, but the country writing to your grandmother, saying you've got $ 5,000, but you got to send me a $1,000, you know. And now, this grandmother knows how to do it.

So I think that's the difference in -- I would caution all of you in your Bills you're helping us to develop this, to make sure we guard against that. Thank you.

WICKER: Thank you, Senator Capito. Senator Rosen.

ROSEN: Thank you. I really appreciate the testimony today. I

have a couple of questions, but one thing that nobody has talked about is data center security. So, one of the things that, you know, they're the keeper of all this data that everybody's collecting. So when we think about privacy, we don't often, you're not talking about, where the data is actually stored, how it's stored and protected.

And in Nevada, of course, we're home to some large data store sites. And I want to be sure that, in the framework, that we talk about where it's stored, protecting it from physical attacks and cybersecurity attacks. So my question is, what are some of the ways your organizations think about physically securing these data centers? What they might do? How long they keep the data? And what happens potentially to orphaned data if companies go out of business? It still is stored and even the data security companies have backup, upon backup, upon backup. So how are you going to address this, and the privacy issue?

ESPINEL: I'll start, and then maybe other panelists want to

jump in. So, you know, for our companies, this is the core of what many of them do. Their business models, the business that they're in is protective of security of data. So it's an issue that our companies have thought about for a long, long time. And we are supportive that if there's privacy legislation passed, that part of that privacy legislation actually includes specific obligations --

ROSEN: On securing of data, because it is such an important

issue in this context. It's one that Senator Cantwell raised as well at the beginning of this hearing, and we think it's critically important that it be part, of not just the privacy debate, but we would hope you'd be part of a federal privacy legislation.

(UNKNOWN): Senator, if I could jump into it. I'd just build on

that. You're noting at a central point, ee look at this as a centrally -- a supply chain management issue. It's the porousness of the digital media marketing, advertising services supply chain that creates these problems. In that sense, you cannot separate security from privacy, even though they are two different things, so you have to put them together.

One of the mechanisms that we've built with our sister trade associations is called the Trustworthy Accountability Group. It is based on an auditing regime, not just a compliance regime, but an auditing regime to help assure that your supply chain partners are trustworthy when you pass data to them. It's based on auditing, and it's had a demonstrable impact on reduction in advertising-based fraud, delivery of malware, those kinds of things. So we're in favor of building stronger supply chain protections into the law.

ROSEN: And could we please be sure that we talk about orphaned

data as companies go in and out of business. That it is still stored some place.

(UNKNOWN): Yes. It's a very important point. Thank you for

raising it.

ROSEN: Someone else want to answer?

(UNKNOWN): Sure, I'd happy, just jump in, I think you're

absolutely right. We can do a perfect job with privacy protections, but if without data and cyber security, then obviously people's information is vulnerable. And this is one of the great benefits that comes from the generation of cloud computing, and all the great companies now that are offering cloud services, and why you see government moving over more to cloud computing, because it does provide a higher level of cyber and data security.

ROSEN: I want to interject one other thing, do you think it'd

be important for us to label some of these large data centers as critical infrastructure just like we do other parts of our grid. Anyone want to answer that?

ESPINEL: I don't have an answer. I don't think we'd be happy to

think about it.

ROSEN: OK.

(UNKNOWN): And we know you have an IT background, and we'd have

be happy to work with you. I'd also just say, on the notion of data security, we have supported legislation for stronger data security standard since 2013. I think only about a dozen states have laws, and there should be a federal standard.

(UNKNOWN): And just adding on to that, we've long advocated for

federal data security standards -- universal breach notification rules. We think it belongs, as it's the other side of the coin, to privacy for sure. We think that the obligations in it should extend to third parties as well.

DR. HARTZOG: And I'll just jump in and say that while security is distinct in many different ways, it's about the ways we craft rules, then maybe privacy frameworks they're related. So intimately -- I mean it's worth thinking about how the mere appetite for data creates security problems, and how we might think about rules that actually start getting at limiting the appetite, and in collection rules, and collation rules as well.

ROSEN: Thank you.

WICKER: Thank you, Senator Rosen. Senator Lee.

LEE: Mr. Leibowitz, I'd like to start with you. When we look at

the Internet, we were examining something that didn't exist at the founding, but it's important to evaluate what kind of thing it is so that we understand our own regulatory power, relative to that thing. You can analogize it to a channel, or instrumentality of interstate commerce. Even though the Internet didn't exist 250 years ago, channels of instrumentality of interstate commerce, certainly did.

In light of the fact that It's a channel of instrumentality under this theory, how would you describe the scope of Congress's authority over the Internet? Would you describe it as exclusive?

LEIBOWITZ: I wouldn't -- well, I would describe, I guess, the

better architecture, and this goes back to the Commerce Clause. It goes back to Gibbons v. Ogden. Then I would describe the better architecture as a strong federal law, or strong federal laws. We're talking about privacy, but there can be others that sets a single high standard for consumer protection. And, of course, it is integrally involved in interstate commerce.

LEE: State governments, of course, have legitimate interest in

regulating a number of things, things that might, incidentally, touch the internet. So how do we, as a Congress, balance the need to operate on this interstate channel or instrumentality of interstate commerce, while not trampling over their authority?

LEIBOWITZ: Well, that's a fair point. And, you know, we all

believe in stasis laboratories of democracy, but we don't have state-by-state seatbelt laws. We don't have state-by-state FAA laws. California, when it passed its own state law, which proved that lawmakers can protect consumer privacy pre-empted all of the municipal laws that existed.

And so, this would be one place, I think where you want to craft a very strong consumer privacy law that empowers consumers, and gives them more control over their data. But I think you want it to be a single federal standard enforced by State Attorneys General, like your Sean Reyes, so that they can bring cases as well.

LEE: Thank you. That's helpful. There's been a lot of

discussion about the FTC's rulemaking authority. It's a authority under the APA to make rules and carrying the force of generally applicable federal law. Now, when Congress delegates broad regulatory powers to an agency, the subsequent rulemaking can create some unintended consequences, because, what's in effect happening is, that that agency is making a law. And sometimes it can become difficult to reverse the burdensome impact that might have on a particular industry.

Mr. Leibowitz, I'm concerned about overly prescriptive privacy regulations and the impact that they have the potential to have, particularly in the area of competition. You think laws and regulations, and even some rule makings by the FTC could have a potential GDPR-like impact on competition by insulating big market incumbents against competition, imposing additional barriers on entry.

LEIBOWITZ: Well, I think you always worry about any rules, or

any laws that create new barriers to entry. We've seen that with GDPR. I would say that this committee, and we'll see where your legislation comes out, could give any rulemaking authority to the FTC under some guardrails. For example, in COPPA, where you gave some delegation, but a limited delegation, to the FTC.

They weren't allowed to increase the age from 12 to 14 of COPPA, but they were allowed to determine what constitutes sensitive information. So in 2012, when we updated COPPA, because COPPA was passed, Senator Markey was one of the authors, was passed at a time when we didn't really know what the Internet would do. We made precise geolocation a sensitive category of information, but you could also come up with a lot of the sensitive categories of information yourself, if you wanted to do that.

LEE: Right. In some ways, an agency like the FTC could be said,

perhaps to be operating at its best, when it's playing the role of cop rather than lawmaker. The enforcement actions, rather than new rule rulemaking endeavors, can be helpful, and they also help increase rather than diminish certainty within the industry. Would you agree with that?

LEIBOWITZ: Well, it said so. And you, of course, have oversight

with your initial subcommittee over the FCC, and have so for some time. And so, you know the agency well. We think of the agency, or people at the agency think of it, as first an enforcement agency, second in a policy agency, and maybe third, a rulemaking agency when Congress clearly delegates that authority for rulemaking. That's why Congress put the FTC under the Magnuson-Moss Act, which makes it very hard to do general rulemaking without a APA delegation from Congress.

LEE: Thank you very much, Mr. Leibowitz. Thank you, Mr.

chairman.

WICKER: Thank you, Senator Lee. Senator Baldwin.

BALDWIN: Thank you. Mr. Chairman. At the end of Senator Rosen's

questioning, we started to touch on the relationship between data security and data privacy, and so I want to explore that a little bit further to get us started. Dr. Hartzog, in your testimony, you've talked about establishing trust rules, and these rules would help consumers believe that the companies are responsible stewards of their data. And you further described a good data steward, as among other things, protective of users data, meaning they do everything within reason to protect us from hacks and data breaches.

While our hearing today was spurred by stories of data misuse, like the Cambridge Analytica scandal, I am not sure that my constituents differentiate between a company's decision to use their data, or give it to others in ways they didn't expect, or agree to, and a company's failure to keep that data secure from third-party criminals who want to steal it. The folks I heard from were just as outraged by Equifax as they were with Facebook.

So Dr. Hartzog, if you are going to do something aimed at making Americans feel that they can trust these companies with their personal data. Do you agree that setting standards for both security of that data should be part of this conversation on the privacy and unexpected use? And I'm interested also, what other panelists might say about tackling both.

DR. HARTZOG: Sure. Thank you very much, Senator. I absolutely agree that security should be a part of this conversation. It's one that requires a lot of expertise, a lot of technological assistance, and so, we should bring that in and build that in. But I think that it's incredibly difficult as a policy matter to disassociate privacy in security, because they're so related to each other.

BALDWIN: Anyone else wanting to share?

(UNKNOWN): Sure, I agree. I mean, privacy and security of data

are two sides of the same coin, and it's just as important, maybe in some cases, more important in one area where this hasn't come up yet, in the context of this hearing, is also government use. And we've seen time and time again, a lot of very large breaches and hacks of government data, personal information of individuals that have major consequences, and that needs to be part of it, and as well as privacy from the government.

Governments at all levels as, you know, state, local, federal are often making very broad data requests of companies. And it's not always clear how that fits into law, due process, and then also data and cyber security. You don't want case where companies are turning over data to the government just to have it leak out in a hack or something. So that also needs to be addressed as part of this.

BALDWIN: OK.

ESPINEL: All right, can I just one caveat --

BALDWIN: Yes, please.

ESPINEL: -- details to that. So that the companies I represent,

many of them are in the cybersecurity business. It is very important to us. We have long advocated for data breach legislation. We have actually advocated, in this context, that we have legislation on data security be part of this. But I will say that while we think that would be optimal, we would also not want to see privacy legislation not happen.

If say, the security or data breach became the issue, we don't need them to move together. We think that would be best. But our number one priority is strong, clear, consistent, workable, effective, truly strong federal privacy legislation.

BALDWIN: Thank you.

(UNKNOWN): I would fully agree with that. Just add to it that

the whole objective here is, to put customers at the center of all of this. To give them a clear understanding, and expectations around how to how data is being used. And they should have a clear level of confidence around how it's being protected. So the two work together very importantly.

(UNKNOWN): I think there's an important point that you

referenced senator. It's that, where people intersect the most with actual harm, is based on various forms of data breach, not privacy breaches. Its phishing emails. And I don't want to minimize anything about privacy, but I want to say that where people get hit in their pocketbooks right now, are in very simple scams that are based on data leaking to places it should not leak to.

(UNKNOWN): Though I'd also push back that an obsession over

data security harms too much, I think, pulls us away from, I think, a more holistic sort of protection for privacy.

WICKER: I would agree.

BALDWIN: Thank you.

WICKER: Thank you, Senator Baldwin. Senator Young.

YOUNG: I thank our witnesses for being here today. I'm going to

ask a question Mr. Leibowitz, but I will submit it to everyone, so you have an opportunity to respond in writing. But there's two things, I'd like to get to. First one, we'll touch briefly on it. Mr. Leibowitz related to the treatment of different types of information and then, more importantly, I'd like to get to developing a **federal data privacy framework** that doesn't disadvantage our smaller entities, small businesses, and startups, and so forth.

So there are clearly different types of information. There's location tracking information, there's DNA information, there's birth certificates, date of birth, personal identifiers. So Mr. Leibowitz, should Congress create a **federal data privacy framework** that treats the same information differently depending on who has control over that information? Or, should it instead focus on the actual nature of the information, regardless of who is in control?

LEIBOWITZ: So, first of all, Senator Young --

YOUNG: Is that a false choice?

LEIBOWITZ: No, it's not a false choice. But first of all I just

want to say I'm glad you didn't want to ask me about the Indiana Wisconsin game last night. That

would a longer conversation. Anyway, so I think it should be - look, the right approach is technology neutral. We shouldn't obsess about that, as Professor Hartzog mentioned, but that's the right approach. It shouldn't be about who collects the data, but what that is collected, and how it's used, because from the perspective of the consumer, that's what they care about. And that's what they should care about.

YOUNG: So how it's used, I would infer from that, that is very

much related to who controls the information.

LEIBOWITZ: That's correct.

YOUNG: OK. All right. Thanks. Again I'll give all of you an

opportunity to respond in writing. So the next one I'm questioning, you're anticipating -- so a post-GDPR, there's actually an economic working paper, again a working paper, so it's it's not done yet. But it appears to indicate there's been a significant drop in investments in startups, small businesses, and the like, post-GDPR. While at the same time, large incumbent enterprises have increased their market share

Now, if in fact, this turns out to be the case, and we continue to get more information that reinforces this dynamic, it seems that we might, too, run the risk of harming small businesses, and new startups, and further entrench larger incumbents for years to come, if we create a federal privacy law that's difficult and burdensome to comply with. So, how best can we tailor standards, so that small businesses and startups aren't disadvantaged by fire nuisances good?

(UNKNOWN): So I would say a few things. One is, for truly small

businesses, you may want to think about some limitation or some exemption. The FTC report that I referenced, and from 2012, talks about data protection and privacy protections in the context of both the transaction and the entity that's doing the collection. So you would treat Amazon differently than you would treat a chain of local markets, for example, and that's one way you can do it.

But I absolutely agree with you, and we want to work with this committee as you move forward with the legislation. But I absolutely agree with you that you don't want privacy legislation to have anti-competitive effects, and that's critical as you move forward. And we have seen, it's early reports, but we have seen, as you pointed out, evidence of barriers to entry, and for new entrants, and in Europe as a result of GDPR.

YOUNG: We'll just go down the line, because I can't see your

name tags. I'm one that we removed from you.

(UNKNOWN): Yes.

(UNKNOWN): Thanks, Senator. You're absolutely right. And this

is a major consideration that we have to have. You don't want to create a regulatory mode over -- you know, that protects incumbents, and you need to come up with a standard that sets companies up of all sizes to be successful, and provide the privacy and security that people want.

(UNKNOWN): Retail industry is one of the most competitive

industries that exists. We thrive in competition. We believe we should exist everywhere. You need to take into consideration the impact on small business, so we're breathing lots of innovation into the whole ecosystem.

YOUNG: Any specific thoughts about how we might do that? I know

it's a difficult question, and how we might fill our standards to -- ?

(UNKNOWN): I think it's acknowledging that some businesses are

not a risk. Some businesses, the kinds of information that they collect, may not be of great risk. Looking at it that way, not just on size, but on the types of data that they have. How much they transact in data.

YOUNG: OK.

ESPINEL: I mean, obviously, you don't want to create a

situation where small companies can violate privacy, or create some sort of perverse incentive to organize and collect and keep your data in a governance structure that would allow people to take advantage of that. But it is also true that we don't want to harm innovation, and we don't want to

harm small businesses. So I think it's something we should definitely be taking into account in terms of, you know, what we believe should be in strong federal privacy legislation.

We think that it would be well within the ability of small businesses to do so. We think we've crafted a proposal that would allow that, but it's an important issue, and it's one that everyone should keep in mind.

(UNKNOWN): Senator, one answer to that is, quite clearly to

spell out, as we've been arguing in a new paradigm, a series of activities that are prohibited, and activities that are allowed. So use of data for red-lining, or discrimination should be prohibited. Sending use of data to send dog food ads to to dog owners, or presumed dog owners, it's not very harmful. In fact, it's beneficial to them. We think that should be allowed.

YOUNG: So, I would just note that I think that even --

WICKER: The dog food lobbyists will love to hear that.

YOUNG: I would just note that I think that even small

businesses, of course, are capable of significant privacy harm and what's good for sectors of the economy might not be a net good for all of society. And so, I think that while -- I think that there are ways to, sort of, craft exemptions for small businesses. What it means is, if you don't want to pay the cost of admission, then you don't get to collect the data. You don't get to do the things that make us vulnerable. And I think that for businesses that are willing to accept that cost, that would work.

WICKER: All right. Thank you Senator Young.

YOUNG: Thank you.

WICKER: Senator Cruz.

CRUZ: Thank you, Mr. Chairman. Thank you to each of the

witnesses for being here today. Thank you for your testimony. Mr. Leibowitz, let me start with you. You spent a number of years leading the FTC. Just today, the FTC announced a task force directed at high tech giants, directed at both anti-trust issues, and consumer protection issues in the tech sector. In your judgment, is that a good idea? And if so, what should they be focused on?

LEIBOWITZ: I would say, it is a good idea. You were at the FTC

when they did a pharmaceutical task force, and that resulted in enormous benefits for consumers, and for competition. I think this is very, very similar and modeled on that effort, and I think they should - well, I'll let the new, we'll let the current FTC figure out what they want to do.

But I think this is a great announcement, and I think they should they should use all of the authority of their agency to see whether there are any anti-competitive behavior in tech companies. I assume that's what they're doing.

CRUZ: One issue that I've been very concerned about, and then I

found Texans and people across the country are concerned about, big tech using its power to engage in political censorship, to silence voices with which they disagree, and to amplify voices with which they agree. To what extent, and I'm going to ask this just to any of the witnesses in the panel who care to respond? To what extent do you consider that to be problematic? And if so, what are the remedies to it?

(UNKNOWN): I'll jump in here senator,, if that's all right.

When I look at the Internet and in our platforms, I do see them as one of the greatest places for free speech and open expression anywhere. And particularly as you look to conservative voices, they've found an audience online. And there are countless examples of individuals, who maybe wouldn't have been picked up at a newspaper, or even on a "Fox News" who are able to build audiences of millions and millions of people, and become household names. And then later, get picked up on TV programs, because of the Internet. And it does provide incredible opportunity for all Americans, and I don't necessarily think you'd want to see the government stepping in to regulate speech there.

(UNKNOWN): Well, I agree with that, and going back to the tech

task force. You know, one of the other tools in the FTC's arsenal is, of course, the 6(b) Study, which is the industry-wide study where it just brings to public life, the way that an industry is focusing, or the way industries are operating. And I suppose, one possibility, as they're looking at a potential 6(b).

CRUZ: Well, and let me amplify that, because one of the most

frustrating things about dealing with the question of tech censorship, is that it is all marked in darkness and obscurity, there is no transparency whatsoever. Both this committee and the Judiciary Committee, on which I also sit, have repeatedly asked tech companies, even basic bare-bones data, in terms of how many speakers on their social media platform, are they silencing?

To what extent are they engaging in shadow banning? And shadow banning by its nature has been reported to be a process where a particular speaker is silenced, but that speaker doesn't know it because they send out a tweet. They send out a post. They appear to be communicating. And yet, the tech platform does not allow those, including those who have affirmatively opted and chosen to hear that speaker, simply doesn't allow them to hear that speaker, and those words, that speech goes into the ether.

And what is deeply frustrating is they have never once, to my knowledge, answered the question, are they doing it? To what extent is it widespread? To what extent is it politically targeted? How do they assess who they will silence? That is a degree of power handed to a handful of tech billionaires in California to monitor and police, and put not just a thumb, but all five fingers of fist in their foot, on the scales of the political discourse.

Let me ask this committee, a 6(b) Study, I think Mr. Leibowitz, is a good potential tool. I see other potential tools. I think the Department of Justice ought to be looking at this question very closely. But let me ask that ask the panel if the objective is more transparency, knowing what, in fact the tech companies are doing, and to what extent they are engaged in active, systematic, deliberate, bias censorship. What tools does Congress have, or the Executive Branch have to ensure more transparency?

(UNKNOWN): Senator, transparency is important, and there always

can be greater levels of transparency. I will say that these platforms seek to serve all Americans regardless of political views, and are open platforms to do so.

CRUZ: I had a curiosity based on one, because I can tell you

when Facebook testified before this committee, and I submitted questions to Facebook about the extent to which they were censoring people, they essentially refused to answer those questions. And I asked Mr. Zuckerberg before this committee, if Facebook had ever once silenced people on the left? Or, if it was only people on the right? And he was unable and refused to answer those questions either. So, sort of, an amorphous commitment to everybody in the universe. When some people are being silenced and others are not, that rings a little hollow.

(UNKNOWN): Each platform has different set of community

standards that perhaps we could do a better job of making it more clear, and more transparent on what they are, and certainly mistakes are made. Sometimes, with voices on the right, but mistakes are often made with voices on the left.

CRUZ: Can you give me an example?

(UNKNOWN): Not off the top of my head, but I --

CRUZ: Nobody else can either. That's the lack of transparency

right there, and one debates these issues using anecdotes, anecdotes are not a very good way to debate an issue. But the reason you're forced to use anecdotes is, because there are no data. There is no evidence. There are no objective numbers. because of the lack of transparency. Thank you.

WICKER: Thank you, Senator Cruz. Senator Cantwell has informed

me that she has no follow-up questions and neither do I.

So, the hearing record will remain open for two weeks. During this time, senators are asked to submit any question for the record. Upon receipt the witnesses are requested to submit their written answers to the committee as soon as possible, but no later than Wednesday, March 13, 2019.

We want to thank our distinguished witnesses, and talented witnesses for a very, very good hearing. I appreciate it very much and the hearing is now adjourned.

END

Feb 28, 2019 17:22 ET .EOF

-0- Feb/28/2019 22:22 GMT