Bloomberg GOVERNMENT

Senate Commerce, Science, and Transportation Committee on Consumer Perspective: Policy Principles for a Fede..,sked FINAL

May 3, 2019 6:09PM ET

TRANSCRIPT

May 01, 2019

COMMITTEE HEARING

SEN. ROGER WICKER, R-MISS.

SENATE COMMERCE, SCIENCE, AND TRANSPORTATION COMMITTEE ON CONSUMER PERSPECTIVE: POLICY PRINCIPLES FOR A FEDERAL DATA PRIVACY FRAMEWORK.

Bloomberg Government

Support: 1-877-498-3587

www.bgov.com

SENATE COMMERCE, SCIENCE, AND TRANSPORTATION COMMITTEE ON CONSUMER PERSPECTIVE: POLICY PRINCIPLES FOR A FEDERAL DATA PRIVACY FRAMEWORK.

MAY 1, 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:

MS. HELEN DIXON, DATA PROTECTION COMMISSIONER, REPUBLIC OF IRELAND

MS. NEEMA SINGH GULIANI, SENIOR LEGISLATIVE COUNSEL, AMERICAN

CIVIL LIBERTIES UNION

MR. JULES POLONETSKY, CHIEF EXECUTIVE OFFICER, FUTURE OF

PRIVACY FORUM

MR. JIM STEYER, CHIEF EXECUTIVE OFFICER AND FOUNDER, COMMON

SENSE MEDIA

(CORRECTED COPY - CORRECTIONS THROUGHOUT)

WICKER: Today the committee gathers for another hearing on Consumer Data Privacy.

I'm glad to convene this hearing with my colleague Ranking Member Cantwell and I welcome our witnesses and thank for appearing today.

Ms. Helen Dixon, Ireland's Data Protection Commissioner, Mr. Jules Polonetsky, CEO of the Future of Privacy Forum, Mr. Jim Steyer, CEO and Founder of Common Sense Media and Ms. Neema Singh Guliani Senior Legislative Counsel for the American Civil Liberties Union. Welcome to all of you.

Consumers are the bedrock of our economy. Through the consumption of goods and services, consumers drive economic activity; power job creation; and create opportunities for innovation, and economic advancement in the United States and around the world.

To foster relationships with consumers, businesses have historically collected and used information about their patrons. The collection of data about consumers' likes, dislikes, and commercial interests has ultimately served to benefit consumers in the form of more customized products and services, and more choices at reduced costs.

Consumer data has tremendous societal benefits as well. In a world of "big data" where physical objects and processes are digitized, there is an increased volume of consumer data flowing throughout the economy.

This data is advancing entire economic sectors, such as health care, transportation, and manufacturing. Data enables these sectors to improve their operations, target resources and services to underserved populations, and increase their competitiveness.

The consumer benefits of a data-driven economy are undeniable. These benefits are what fuel the vibrancy and dynamism of today's Internet marketplace. Despite these benefits, however, near-daily reports of data breaches and data misuse underscore how privacy risks within the data-driven economy can no longer be ignored.

The increased prevalence of privacy violations threatens to undermine consumers' trust in the Internet marketplace. This could reduce consumer engagement and jeopardize the long-term sustainability and prosperity of the digital economy.

Consumer trust is essential. To maintain trust, a strong, uniform federal data privacy framework should adequately protect consumer data from misuse and other unwanted data collection and processing. When engaging in commerce, consumers should rightly expect that their data will be protected.

So, today, I hope witnesses will address how a federal privacy law should provide consumers with more transparency, choice, and control over their information to prevent harmful data practices that reduce consumer confidence and stifle economic engagement.

To provide consumers with more choice and control over their information, both the European Union's General Data Protection Regulation and the California Consumer Privacy Act provide consumers with certain privacy rights. Some of these rights include the right to be informed or the right to know, the right of access, the right to erasure or deletion, the right to data portability, and the right to non-discrimination, among others.

I hope witnesses will address how to provide these types of rights within a United States federal framework without unintentionally requiring companies to collect and retain more consumer data. Provisioning certain privacy rights to individuals, without minimum controls, may have the opposite effect of increasing privacy risks for consumers.

In developing a federal privacy law, the existing "notice and choice" paradigm also has come under scrutiny. Under notice and choice, businesses provide consumers with notice, typically through a lengthy and worthy privacy policy, about their data collection and processing practices. Consumers are then expected to make a "take it or leave it" choice about whether or not to purchase or use a product or service, but is this really a choice?

I hope our witnesses will address how to ensure that consumers have access to simplified notices that offer meaningful choices 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 bury an organization's data collection activities.

I also hope witnesses will speak to ways in which Congress can provide additional tools and resources for consumers to make informed privacy decisions about the products and services they choose to use both online and offline.

Fundamental to providing truly meaningful privacy protections for consumers is a strong and consistent federal law. This is critical to reducing consumer confusion about their privacy rights and ensuring that consumers can maintain the same privacy expectations across the country.

I look forward to a thoughtful discussion on these issues and again welcome all of our witnesses.

And I now recognize my good friend and Ranking Member, Senator Cantwell.

CANTWELL: Thank you, Mr. Chairman.

And thank you to the witnesses for being here today on this important hearing about how to develop a federal data privacy framework. It's essential that we give a front row seat to the consumer advocate perspective and that's what today's conversation does.

When the dust settles after a data breach or misuse of data, consumers are the ones who are left harmed and disillusioned. In the two months, since our last full committee hearing on privacy, consumer data has continued to be mishandled. It's clear that companies have not adequately learned from past failures and at the expense of consumers, we are seeing that self-regulation is insufficient.

Just days ago, cyber security researchers revealed existence of a massive Cloud data breach left wide open and unprotected containing addresses, full names, dates of birth, income, marital status on more than 80 million U.S. households. This blatant disregard for security and privacy risk makes it clear why we are here today.

Microsoft recently admitted that an undisclosed number of consumer web e-mail accounts were compromised. We learned more about privacy lapses on Facebook and two more third-party Facebook apps exposed data on Facebook users revealing over 540 million records including comments, likes, account names and Facebook IDs.

So, Mr. Chairman, how do we create a culture of data security that protects consumers and allows commerce to continue to grow?

Consumers continue to be bombarded by threats to their privacy, cyber security, adversaries become more sophisticated and more organize day by day and we really need to understand privacy on a continuum of data security. We need to make a more proactive approach to cyber security and make sure that we are continuing to protect consumers.

These become especially important in the age of Internet of Things. Yesterday the Security Subcommittee considered this issue at length. Billions of devices collecting data about consumers at all times, means there's billions of entry points in large surface areas for cyber attack.

We learned more about new botnet attacks and now weaknesses almost daily. And we face serious questions of how supply chain vulnerability which is reminding us about how security here in the U.S. is dependent among the health of our Internet -- Internet cyber security. Members on our side of the aisle even had a secure briefing on the potential threats and impacts to our own devices.

So, it is important to remember that the Internet is a global network, no matter how secure we make our networks remain vulnerable to weaknesses abroad. That is why it's essential that we have a national strategy to deal with these threats.

We also need to work with our international partners to form coalitions around cyber security standards and work towards harmonizing privacy and cyber security regulations. This latest privacy and security bridges in advancing cyber threat show that this problem is accelerating.

But as you said Mr. Chairman, there is also lots of opportunity for great applications of services and devices that we all like. So, it illustrates the complexity of the challenges we face.

Consumers are at the center of this and we cannot just require them to have a deeper understanding of the risk involved. We need to make sure that their devices and concerns are not just about noticing consent. But we have strong provisions here and in description that will help create a better culture.

The best plain language notices, the clearest opt and consent provisions, the most crystal clear transparency doesn't do any good one, companies are being careless or willingly letting our data out the back toward the third-parties that have no relationship to the consumers.

While the benefits of the online world are everywhere and I truly mean that everywhere so must be the protection of personal information that is more than just a commodity. We need to make sure that the culture of monetizing our personal data at every twist and turn is countered with the protection of people's personal data. So, Congress has to come to terms with this.

I know that the members of this committee are working very diligently on trying to address that. And that we are working to try to make sure that the things that happened in the 2016 election cycle also don't happen in the 2020 cycle.

With these issues of information being stolen or manipulated or in trying to influence or disrupt the governments, even our own hacking of our employee personal information accounts, show that we are vulnerable and that we need to do more.

So, the consistency of the hearings that we've had on this issue, I appreciate both Chairman Thune and you having these hearings about cyber security, about Equifax, about cyber hygiene and what we should be doing, this all I believe should be part of the solution.

Data security for Americans means that we extend the protections and we make sure that the online world is operating in a way that we see, are helping to protect consumers in individual information.

So, Mr. Chairman, I know that you remain very dedicated to comprehensive legislation here, I do as well. Even though the challenge is high. We need to have the opportunity to craft solutions that address security and privacy for the entire life cycle of our data and collection to storage and to processing.

So, hopefully today today's hearing will give us more input as the way consumers look at this issue and what we can do to help us move forward.

Thank you.

WICKER: Thank you very much Senator Cantwell.

And again, we welcome our witnesses. Your entire statement or statements will be included in the record and we ask each of you to summarize your opening statements within five minutes.

So, we'll begin down at the center of the table with Ms. Dixon. Welcome.

DIXON: Chairman Wicker, Ranking Member Cantwell and members of the committee. Thank you inviting me to be here today.

I'm pleased to have the opportunity to share with the committee the experience of the Irish Data Protection Commission in dealing with complaints from consumers under EU Data Protection Law and hope would be of assistance in your deliberations on a federal privacy law.

As the committee is aware, I submitted an advance is likely more expand a written statement to that my five minutes today represent, so a suggestion by the Chair I will cover all its key points for you briefly now. An important context in talking about the EU Data Protection Law is a fact that the right to have ones personal data protected existence and explicit fundamental right of EU persons -- under the EU charge of fundamental rights.

It is the case then that the right to data protection in the EU exists in all personal data processing context and not just in commercial context. The committee is well aware I think at this stage of the basic structure of the EU GDPR which sets like firstly obligations on organizations than rights for individuals and finally provides for supervision and enforcement provisions to be implemented by independent data protection authorities. As an EU regulation it is direct affect in every EU members state.

The obligations on organizations processing information that relates to an identified or identifiable person are set down in the series of high level technology neutral principles. So, principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability.

The GDPR contain some prescription around new accountability provisions and in particular requirements in certain cases to now were pointed data protection officer. In addition does an obligation to notify breaches of personal data that give rights to risks for individuals and to the data protection authority within 72 hours of the organization becoming aware of the breach.

In turn, then the individuals and consumers whose personal data are processed have a series of enumerated rights under the GDPR. This cover the right to transparent information, the right to access to a copy of their personal data, the right to ratification, the right to erasure and so on. And each of these rights is very in conditions pertaining to the circumstances in which those rights can be exercise.

Finally then, the GDPR provides for independent and adequately resource to data and protection authorities and EU members state. As data protection authorities leave a very broad range of tasks that range from promoting awareness, an issue in guidance on data protectional (ph). To encouraging industry codes of conducts, to handling all valid complaints from consumers and then investigating significant infringements of the GDPR.

The new one stop shop for multinationalism to the GDPR means that the Irish Data Protection Commission is the lead supervisory authority in the EU for the vast majority of U.S. global Internet companies, such as Facebook, Twitter, WhatsApp, Google, Airbnb and Microsoft as this have their main establishment in Ireland.

The GDPR has introduced a much harder enforcement edge to EU Data Protection Law with the range of corrective powers of the disposal of data protection authorities, in addition to a capability to apply fines of up to 4 percent of the worldwide -- worldwide turnover of multinationals.

In the 11 months since GDPR came into application, the Irish Data Protection Commission has received an excess of 5,900 complaints from individuals. Its frequent (ph) to a feature of the complaints we handle from consumers that their interest in their personal data is as means of pursuing further litigation reaction.

So, for example, former employees of organizations often seek access to their personal data as part of the pursuit of an unfair dismissals case, consumers may seek access to CCTV images in various different scenarios to pursue personal injuries cases and so on.

Overall, the most complaint against sectors in a commercial context are retail banks, telecommunication companies and Internet platforms.

On my written statement just provide you -- provided you with some specific case studies and examples of the complaints we've handled.

Equally worth mentioning is the complainant's to my office have rights to appeal and judicially review decisions of the Data Protection Commission. And my office is involved in over 20 litigation cases currently before the Irish courts.

And the committee might be interested to know that the vast majority of decisions appeals to court from my office relate to disputes between employers and employees and far fewer relate to commercial context.

Aside from handling complaints, the Data Protection Commission has power to open investigations of its own volition and we have 51 large scale investigations underway at covering the large tech platforms amongst each others.

So, in conclusion, EU data protection law places a very strong emphasis on the individual in light of the fundamental rise and strong emphasis on the exercise of the rights of the individual and accordingly it mandates the handling of every complaint from an individual by Data Protection authorities.

This means that EU Data Protection authorities play an important jewel role on the one hand resolving high volumes of issues for individuals and on the other supervising companies to ensure systemic issues of noncompliance are rectified and punished as appropriate.

The GDPR is 11 months old at this point and clarity and consistency of standards will evolve in the coming years driving up overall the standards of protection for consumers in every sector. Thank you.

WICKER: Thank you very much, Ms. Dixon.

Mr. Polonetsky?

POLONETSKY: Thank you, Chairman Wicker, Ranking Member Cantwell, committee members.

Eighteen years ago I left my job as the New York consumer first commissioner to become one of the first waves of chief privacy officers when that was yet a novel title.

Today, as CEO of FPF, I work with the CPOs of more than 150 companies with academics, with subsociety and leading foundations on the privacy challenges post by tech innovations.

I first testified before this committee almost 20 years ago to address privacy concerns around behavioral advertising. And almost every day since, we've seen those reports of new intrusions, new risks, new boundaries crossed. Sometimes, it's simply a company being creepy; sometimes it's a practice that raises serious risks civil liberties or our sense of autonomy.

It's long past time to put a privacy law in place that can support that trust that Americans should have when they use their phones, when they surf the Internet, when they shop online, all the activities of daily life. Every day we delay it becomes harder. New businesses launch, new technologies are developed and become entrenched.

At the same time, we are of course benefiting from many of these technologies as you both mentioned, companies reinventing mobility and making transportation safer, machine learning has been built into so many of the products and services, health care diagnosis, education tech providers working on personalized learning. Every one of this holds great promise, every one of them also brings new perils.

It's a global challenge of course in almost every leading economy, not just our European colleagues put comprehensive laws in place. Japan, we should take special note perhaps of the APEC CBPRs, the Asia Pacific region where the U.S. has played a long role in which we've recently committed to and the proposed treaty for trade between U.S.-Mexico and Canada.

We shouldn't be left behind as the standards that are actually defining technologies today and the terms of trade for decades to come are being established, even small businesses do business globally today via the web and need that guidance.

So, baseline law should have strong protections matching and exceeding the key rights of California's privacy law, transparency, access, deletion, the right object, protections for minors, the right to object to sales of data, but we also need to add some of the other core privacy principles that aren't included in CCPA.

Compatible use context special restrictions on sensitive data, the full range of fair information practices as they've been reflected in so many of the national and international models and many who originated back in the 1970s in the U.S. should be in our law.

In drafting, we should be clear about what is covered if we don't know what's personal, we don't know what's in and what's out, but our view that this isn't a binary in or out decision. Information isn't either completely explicitly personal and it's probably never completely anonymous.

There are stages of data and a law that is careful would nuance different levels of rights and restrictions based on whether data is fully anonymous, whether it's pseudonymous, the actual different stages in the lifestyle are the best way to match the corresponding requirements.

Research hasn't always been handled well in a number of the legislative models around the world. We want to, I think, encourage beneficial research if it is being carried out in a way that supports privacy, fairness, equity, the integrity of the scientific process.

We should encourage research when the appropriate ethical reviews are in place. And at the end of the day, internal accountability mechanisms are how organizations actually make sure they follow the law. We don't want just privacy in the law. We wanted on the ground. We want privacy by design and that means employees that are trained, that means tools and systems that support responsible data stewardship.

So, law should encourage comprehensive programs and whenever possible, we should incentivize PETs, Privacy Enhancing Technologies that deliver us perhaps the benefits of data while making sure that we have strong mathematical proofs that we'd minimized any risks. And of course, any law is going to impact these sectoral state privacy laws that have been passed in recent decades.

We certainly should avoid a framework where our website operator or small business should have to deal with complexity of inconsistent state mandates on many of the day-to-day issues of operating a business. But these concerns can be reasonably avoided with carefully crafted federal preemption. There are clearly core state privacy laws that can and must exists, student privacy laws and others and that I think is an important challenge for the committee.

But laws are only as good as enforcement, the FTC should have not only the civil penalties, not only the careful targeted rulemaking but it also should have education and outreach so that new businesses understand, can get their questions answered. The FTC needs both the carrot and the stick. And of course, (inaudible) who have been such critical partners to our federal leaders should continue to have a role.

Thank you for the chance to share those thoughts with you today.

WICKER: And thank you very much, sir.

Mr. Steyer?

STEYER: Thank you, Chairman Wicker, ranking member Cantwell and the distinguished members of this committee, it's great to be here.

I'm Jim Steyer, I'm the founder and CEO of Common Sense Media. We're the leading kid's median tech group in the United States. We're launched about 15 years ago. Just for a little background, we have 110 million unique users every year on our consumer platform. We created award winning Digital Citizenship Curriculum, that's most in school in United States.

And we have 75,000 member schools across the world, most of them in the U.S. teaching kids about not just their privacy rights but the safe responsible use of tech. I'm also at profit Stanford where I've taught constitutional over the last 30 years.

The one thing I'd sort of say in general today is that someone has been a child advocate for 30 years and the father of four, I've got a 15-year-old, that's our youngest now. I think this is a major moment in time on -- it's been literally almost 20 years since the U.S. -- anything meaningful in the area of privacy.

And right now, even though there are tens of millions of American families who are worried about privacy issues for themselves but most of all for their children, there's only one, the state that I live in California that has comprehensive privacy law. And in fact, it was -- Common Sense Media, who spearheaded that law last year, that CCPA has been referred to.

I just think it's this great moment in time where this body has to act. I always say when I get up in front of parents that, you know, 20 years ago, Mark Zuckerberg was barely (inaudible). Google was a concept in sort of -- obscure math ideas and this device didn't even exist. But it's all here now and our kids are living on it and we're all living on it.

And so during this time of extraordinary growth in the tech economy, we have got to come up with a comprehensive, smart, common sense privacy law that's going to protect all of us, all of our families and most of all, our kids.

Right now, there essentially are no guard rails when it comes to privacy federally. We have one law, the California law that we pass last year, goes back into January, and then we have GDPR which Ms. Dixon referred to.

So, it's high time that Congress and this body stepped up to the place and protect the fundamental privacy rights of every citizen in this country.

The one thing that we saw very much in California when we pass the law is that it is a totally bipartisan issue. This is something that everybody ought to be able to agree on because we all are both the beneficiaries of the extraordinary aspects of the tech industry but we're also the victims when privacy rights are violated, whether it's individually or whether it's involves interference with our electoral process.

So, overwhelming majorities of America, Americans agree with us, the California law pass unanimously and so I would just urge you to really work as you do as a bipartisan group to support comprehensive privacy laws now.

Four big points that I would say to you.

One, the California law is a floor not a ceiling. Anything that should come out of this committee and this Senate should be stronger than the California law. I know we negotiated it. We gave up a number of rights in order to get it pass. We work with companies like Microsoft, Apple and Salesforce to get it done. But this body should be looking at California as an absolute floor rather than as a ceiling.

The second thing I would say is that kids and teens are the most vulnerable. They deserve special protection. As our good friend Senator Markey knows as well as anyone, kids need extremely important and unique protection. So, as you consider the law, we hope you will put kids first and include teens in this law as well.

Third, there needs to be an ongoing public education, public awareness campaign. The average American, I would argue the average senator is not a computer wizard or tech wizard. So, we need simple -- once we have a law, we need to explain it to the public how to use it. That's a big thing we're going to start doing in California in 2020 but I would urge you to think about that. How do you make it simple, easy, and easily understandable for -- like me and some of you.

And last but not the least, I do want to raise the other thing. In the wake of the live streaming of mass shootings on Facebook a few weeks ago, the inability of YouTube and other platforms to pull some of that extraordinarily and appropriate content for anyone let alone children down. We would urge you to think about it separately. The concept of Section 230 in the safe harbor provision and what kind of regulations there ought to be for kids in particular inappropriate content on the web.

At the end of the day, I think the bottom line is clear. This is your folks' moment to do something great for everybody in America on a bipartisan basis and we are happy to help. Thank you very much for having me.

WICKER: Thank you very much Mr. Steyer.

Ms. Guliani?

GULIANI: Thank you for the opportunity to testify today on behalf of the ACLU.

We're all here because the current privacy regime is broken and it's failing consumers. Lack of privacy affects everyday life. It can increase unfair discrimination, exacerbate economic inequality, and even threaten physical safety.

For example, studies have documented how some retailer charged customers different prices base on things like their ZIP code or their browsing habits. In many cases, consumers aren't even aware their information is being collected much less how they can protect themselves against these types of uses.

In another study, online mortgage lenders charged black and Latin borrowers more and higher rates for their loans. Replicating the types of discrimination that federal laws like the Equal Credit Opportunity Act were designed to prevent.

The ACLU strongly supports federal privacy legislation to address problems like these. There are many elements that such legislation should include but I want to highlight four areas in particular that are of concern.

The first is any federal law should be a floor not a ceiling. Some industry representatives have urged you to broadly preempt state laws as part of any federal legislation. I want to be crystal clear here. This would be a bad deal for consumers. If Congress uses federal privacy legislation as an opportunity to broadly preempt state laws, it would cause more harm than good.

As an organization with affiliates in every state, the ACLU has been at the forefront of many efforts to pass strong state privacy laws. We know firsthand that in many cases it has been states, not Congress that have led efforts to protect consumers.

California was the first state in the nation to require customers -- to require companies to notify customers of a data breach. And just last year, it passed a broader consumer privacy bill that you've all -- that you are all familiar with. Illinois has set important limits under the commercial collection and storage of biometric information and nearly all states regulate unfair and deceptive trade practices, complementing the FTC authority in this area.

These states have acted as laboratories, they've experimented and innovated with new ways to protect consumers. We should be weary of the federal government stepping in and with one stroke of a pen wiping out dozens of state laws already on the box and preventing future ones.

Broad preemption in fact would represent a shift in the approach taken by many federal laws. HIPAA allows states to enact more stringent protections for health information and Federal Civil Right Laws have historically allowed states to pass higher standards. This is one of the reasons we have state laws that protect against discrimination on the basis of sexual orientation despite the gaps in federal law.

Federal legislation must certainly account for cases where it would be impossible to comply with both state and federal law. But that can be accomplished through a narrow and clear preemption provision that addresses conflicts and explicitly preserves the rights of states to pass stronger laws and to enforce those laws. Two, any privacy legislation should allow consumers to sue companies to violate their rights.

The FTC undoubtedly needs more power and more resources. But even if its size were doubled or even tripled there would be giant enforcement gaps. This is part of the reason that the California Attorney General recently supported legislation to strengthen California's law with a privacy right of action.

In discussing the legislation, he said, "We need to have some help". He highlighted that individuals should be able to enforce their rights in cases where the government was not able to take action. Poll in California's found that 94 percent of consumers support being able to take a company to court if their privacy rights are violated.

Three, legislation should protect against discrimination. There must be the resources and the technical expertise to enforce existing federal laws that prohibit discrimination and the housing credit and employment context.

In addition, however, federal law must be strengthen to prohibit advertisers from offering different price, services and opportunities to individuals based on protected characteristics like race and gender. And consumers must also have the tools to address algorithms or machine learning tools that desperately impact individuals on the basis of such protected characteristics.

Finally, there should be guardrails on how data can be collected, stored and used. For example, use of information should be limited to the purpose for which it was collected, unless there is additional and foreign consent. And we should also prohibit so-called pay-for-privacy schemes that there into create privacy have and have nots. And risk causing disastrous consequences for people who are already struggling financially.

Without these protections, a new federal law risk being a step backward not forward. I look forward to answering your questions.

WICKER: Well, thank you very, very much. And we'll now proceed to questions.

Mr. Polonetsky, let me begin with you. And I refer to this in my opening statement. Was the GDPR and the CCPA are written to give consumers more control over their data by establishing certain rights. These rights include the right to access to erasure or deletion right, to data portability and others.

I mentioned in my opening statement a concern that these rights may inadvertently decrease privacy for consumers because companies maybe compelled to retain track or re-identify data that they would otherwise have discarded. So, if you would comment about that and then I'll ask the others if they've got any observations.

POLONETSKY: I think we can effectively provide people strong rights of access and deletion if we carefully make it clear that we're not going to be requiring companies to more tracking in order to be able to provide that data.

Certainly GDPR goes in that direction and I think it's solvable but making it clear that you need to know who you are providing data to, you need to clearly verify so that you're providing the data to the person and not creating an opportunity for data breaches.

But I think carefully crafting the right in a way that gives us those protections is quite feasible.

WICKER: Is that a problem that has been experience standard GDPR? I just didn't understand exactly what you were saying there.

POLONETSKY: GDPR certainly makes it clear that you aren't -- obligated to do extra tracking in order to have the data to provide back to people. I think there's been some concerns since CCPA is new and exactly what it means to verify somebody isn't quite clear. So, people are looking for guidance.

I think one of the reasons I argue this committee should act and indeed override CCPA is we can fix some of those areas where there is clarity so that people have a strong right of access. And we don't create any over disposure by providing those deletion rights that we want to provide.

WICKER: OK, Mr. Steyer.

STEYER: So, thanks Mr. Chairman. I had couple of things. One, in California, few years ago, we passed the bill called the eraser button. And the point was you could erase -- kids under the 18, could we have erase any content that they had foolishly posted without thinking about it.

We think that that idea is something that should also be part of a broader federal law. The issues was actually been the enforcement. So, my colleague on my left mentioned the enforcement issues. That's been the biggest issue around the eraser button -- the eraser issue. And actually I'm sure that Ms. Dixon knows that because there's a right in Europe to be forgotten. So, this is a very important thing that the committee should do.

The second thing I've mention of what Jules just said is that data minimization which were again (inaudible) simple minded person like me means that you only should use the data for what you really needed for. You shouldn't be able to use data broadly for multiple purposes, is another critically important element of what a federal privacy law should have.

And that was the toughest part for us to actually hold on to in California. That's the piece of the CCPA that if we -- if you could do it over again and make it stronger, you'd have stronger data minimization.

So, those are the two items that I'd mention, Mr. Chairman.

WICKER: Ms. Guliani?

GULIANI: Yes, I mean I think absolutely. I mean the average consumer doesn't know what data is being collected on them and doesn't necessarily know how to make sure that that data is accurate or to request deletion. So, that's something that can certainly be accomplished while accommodating, I think the interest of not wanting to encourage businesses to retain more information.

I will note that the right to be forgotten is not something that we would want to be adopted identically in the U.S. There are potential First Amendment considerations. For example, we won't want an individual to be able to request that, a newspaper published an article about them that discouraging, take down that content. So, there might need to be some modifications from GDPR and to be consistent with the U.S. constitution.

WICKER: Thank you.

Ms. Dixon, let me shift just in the few moments I have left. There's information that after the GDPR went into effect, a number of small businesses had to shut down because they simply could not afford to comply. Is that a concern? And what do you say to that? What advice do you have for this Congress?

DIXON: I mentioned earlier, Chairman, that the tasks of data protection authorities in the EU are broad. And one of our key tasks in advance of GDPR was to prepare industry and then particular SMEs and microenterprises. And in doing so, we heard a lot of concerns from smaller companies about their ability to comply with what is vast and sometimes technical and complex law.

However, through the awareness campaign that we really dive in the very specific guidance, we were able to issue the smaller enterprises. We were able to clarify the risk-based approach that the GDPR endorses. In other words, that organizations only need to implement what are called the organizational and technical measures appropriates that levels of risk and the scale of personal data processing that they're undertaking.

So, in fact, the GDPR does consider smaller enterprises, some very specific articles in the GDPR like Article 30 the requirements to document data processing operations. It recognizes that smaller scale enterprises don't need to conduct that particular exercise.

So, I think for every organization, the GDPR is a win-win when it's implemented in genders, the trust of consumers that protects organizations. And we haven't seen any direct evidence of organizations having shutdown because they couldn't meet the compliance burden. Once they understood how they could practically implement it.

WICKER: Thank you.

Senator Cantwell?

CANTWELL: Thank you, Mr. Chairman.

Again, thank you everybody for your testimony.

Ms. Guliani, it's good to hear from you and Mr. Steyer about the California law and it's needed for improvements.

I can guarantee you one of the first calls I made when taking over the spot was to Attorney General Bisera, a former colleague to ask him about the California law, and he said, basically what you articulated Ms. Guliani that it needs improvement and that he saw to seek that.

So, I wonder that -- Ms. Guliani, you were very clear on the discriminatory practices in housing and employment, race, gender issues that are being deployed to your point of not -- people not even knowing how the information is used and collected.

Who do you think is the repository for all of these violations that are existing today? Do you think we get that from you, the AGs, the -- like who do you think has the running list and duplicity's actions that are being use against people with their data?

GULIANI: So, we don't -- I don't think anybody has a running list which is why I think it's important that we have robust enforcement on multiple levels, right.

WICKER: Yeah.

GULIANI: So, we need the FTC to be resource and have the technical expertise. They should also be able to level civil penalties. But at the same time, I think we want to take advantage of state attorney generals and regulatory agencies who have a long history of protecting consumers.

And finally, I think consumers have to have the rights to go to court themselves. I mean, there maybe many cases where either state or federal authorities don't have the resources. And so for good reason, can't follow up on a privacy violation.

I think without a multi pronged approach from an enforcement standpoint which we'll effectively have or gaps, and gaps that can be exploited.

CANTWELL: Well, I think to the issues that you mentioned, these are things that we've batted down in other areas of the law. So, to see them pop up online would be really just an undermining of current federal law so that's why it's so important that we fight against it, and to make sure that the online world meets the same standard as broadcasters after meeting the broadcast world or healthcare officials have to meet in another forms of healthcare that we don't allow those things to pop up.

I think the one thing that we learn from the Facebook hearing were Facebook writ large is just that anytime you see a survey online, chances are that information is just a data collection source so that, you know, some information can be used against you or when you have that familiar, do you want to call back from somebody on service is really a -- can I sell your name to someone else who's going to then, you know, try to solicit something from you.

So, I think it's very important that we get a handle on these current privacy violations so that the public has a better understanding, to this point about the erasing of data, one thing that we've learned from our privacy law that we pass through this committee on clearing your good name.

WICKER: Yeah.

CANTWELL: Which was a tool by which we gave those who were victims of identity theft, the ability to get a claim through the FTC and permit, you know, basically present that to law enforcement that they were the victim not perpetrator of the crime.

How do you see enforcement working on something like that, because to me, it's a very big, very big challenge to have, you know, consume, you know, the standard why which we're operating now. It's basically people call attorney generals and attorney generals basically prosecute these people and get them shutdown, really. That's what happens. Consumers call in and complain.

And so in this case, there's a lot of data information being use and they don't even know how it's being use. And they don't even know that that's -- that there, as you said on housing or loans being discriminated against.

GULIANI: Yeah, I mean I think that you really touch on an important point. And one is that it's hard to figure out when a privacy violation has occurred or discriminate -- discriminatory conduct does occurred. I mean just think about discriminatory advertising. I don't know the ads. I'm not seeing. And so how do I know that I've been denied the opportunity for let's say an employment opportunity because I'm a woman or a person of color.

And so, I think that it's really important that one the standards be clear so that companies know the rules of the road, and two, that the enforcement entities need to be looking at those companies following up on those complains when they get phone calls having the resources to do that.

But I think another thing that we also should look at is especially with algorithms and machine learning more transparency. You know, companies allowing outside researches -- researchers to look at their algorithms and say, hey, this is having a disparate impact or this is having a discriminatory effect.

And so, we should really be encouraging those types of behaviors and encouraging companies to do risks assessments to measure potential discrimination.

CANTWELL: Well, just to be clear, you think that these companies should face the same penalties as other companies who have violated the law that's already in existence?

GULIANI: Exactly. Self-regulation is not working and there should be a robust enforcement.

CANTWELL: Thank you.

WICKER: Thank you very much.

Senator Blunt?

BLUNT: Thank you, Chairman.

Ms. Dixon, you mentioned in your testimony that the Irish Data Protection Commission is the lead supervisory authority in the EU for significant number of U.S. companies because of domicile and other things. I want you to name companies but are there U.S. companies 11 months now into the implementation of this that are none compliant with the GDPR?

DIXON: Thank you, Senator. In the 11 months since the GDPR came into application, we've opened 12 significant investigations into potential infringements by large U.S. tech companies. So, we have reason to believe then clearly that there are potential infringements of the GDPR rising.

And we are significantly advanced in a number of those investigations and intend to bring a decision and then I command those investigations.

BLUNT: Do, you have some more investigations with the EU based companies?

DIXON: We do. So, overall, we have 51 significant investigations underway currently. So, subset relates to the U.S. 10 companies. We supervised government and public sector also in Ireland in addition to commercial enterprises. So, it's across the board.

BLUNT: So, it's safe to assume that the regime has been put in place. The U.S. companies don't have a more difficult time or easier time with the one that EU companies in complying?

DIXON: I think it's not a case of a more difficult or easier compliance approach. It's a risk-based approach that the GDPR endorses. And so, when you have platforms that have billions of users in some cases and certainly 100 of millions of EU persons as users the risks are potentially higher in terms of the issues that arise around breaches and noncompliance with the principles.

BLUNT: And both EU companies and U.S. companies are being fined for noncompliance?

DIXON: We will have to conclude the investigations and then...

BLUNT: But for the penalty? So, have you issued any fines up till now?

DIXON: The investigations have to inject concluded the first thronged (ph) that we have underway.

BLUNT: All right. Thank you.

Mr. Polonetsky, Senator Schatz and I have some legislation on facial recognition, thinking that also as a significant data that uniquely recognizes people obviously. I think we both agreed that that information collected through facial recognition it needs to be treated like all other personal data.

Can you share your perspective on how Congress should define personally identified information, whether that that should include facial recognition and how we would treat that in a way similar or unlike other commercially collected data.

POLONETSKY: I argue that a bill should recognize that there are special categories, sensitive categories of information, and the typical default for collecting, using, sharing that information should be a strong consent base model. There may be places where we can see opt out or default but certainly when it comes to sensitive data.

Biometric data, DNA, facial prints, fingerprints are clearly sensitive data and should be subject to a stronger consent base standard.

BLUNT: Are there best practices out there yet?

POLONETSKY: We've done a fairly detailed set of best practices as we've seen these technologies in the market. What we tried to do is differentiate between facial recognition which I think we all know, recognizing my unique ID, creating a template, and then perhaps facial detection. How many heads are in this space, how many male or female heads? Certainly can see the potential for discrimination if I treat people differently but I don't have a unique identifier.

And so, in our structure, we set up a tier if business who just wants to know how people are in the room. Unique numbers of people that might be unnoticed in a way to out a doubt, but if I'm going to identify you by your name, the defaults want to be that I need your permission.

BLUNT: And Mr. Steyer, I think you were at the meeting the other day with senator and I had on the camera, the Camera Act.

STEYER: Right.

BLUNT: Does that -- is there a facial recognition element there or concern about kids on screens?

STEYER: There's a -- there should be, and by the way, thank you very much for supporting the Camera Act because I think this is really an issue that it's a big deal for everybody have we got it. Your personal identify information is really, really, important. The one thing I would say I differ with Mr. Polonetsky, the California law basically doesn't differentiate between types of data. It just says all data deserves strong protection.

And one thing I would urge the committee to think about is look at how California treated data. We didn't actually distinguish, and Mr. Polonetsky wrote thoughtful comments for this hearing. But we think basically, all data, that is your personal data is really important. Obviously, stuff like facial recognition matters a lot to all of this could we understand it. We think all data matters.

BLUNT: Well, thank you and (inaudible) working on the screen time, face time element that particulate that relates to kids and...

STEYER: And thank you for doing here very much.

BLUNT: Thank you, Chairman.

WICKER: Thank you.

Senator Schatz?

SCHATZ: Thank you, Mr. Chairman. Thank you for the testifiers. We've got a constructive conversation. I want to start with the FTC.

My view is that any law ought to have and this is for Mr. Steyer and Ms. Guliani. That any law ought to have first fine authority and EPA rulemaking authority, and I just want to get your view on whether you agree with that, Mr. Steyer?

STEYER: I completely agree with that. I mean, if you really look at it in a practical common sense way, and Mr. -- Attorney General Becerra you guys are referring to, who has angry at me because we passed the law because he's a chief -- he's my law school classmate and friend. Oh my God, now it becomes the chief privacy officer in California. The big issue is resources for enforcement. You could speak to Attorney General Becerra.

SCHATZ: Yeah, I get that. So, it's a yes, Mr. Steyer?

STEYER: Yes, definitely with your question.

SCHATZ: Ms. Guliani?

GULIANI: Yes, definitely.

SCHATZ: And let's talk about resources for enforcement. So, Ireland DPA has 135 employees are about one in a half percent of the U.S. population. The FTC has obviously more employees but as it relates to full-time privacy staff has 40.

WICKER: Yeah.

SCHATZ: Do we need more human beings that the FTC devoted to privacy?

STEYER: Yes, absolutely, no brainer.

GULIANI: Yes, absolutely and increase technical expertise. I think as you note the size of the FTC is probably smaller than the D.C. office have a lot of major tech companies

SCHATZ: That's a fair point. OK. Let me go back to transparency and control. I've been bagging this from -- for a while. I'm great with transparency and control. I just don't think its enough and as we think about Senator Blunt and I working on facial recognition. You're going to lock into a mall and this idea that there will be sensors everywhere, and they will be pinging off your face and then, let's say we pass a pretty robust transparency and control regime.

I'm not sure how you can if actually the transparency and control regime. If your phone is not constantly giving you a notification and having you make individual micro decisions about whether Banana Republic is going to send you a message or the Apple Store or whatever. Or what if you don't -- what if you didn't bring -- I mean, have been. What happens if you didn't bring your phone into the mall, how do you even say no to some of these data collection?

It seems to me that we do need to be built in suspenders. That we ought to be able to turn the deals on somebody's decisions. But we also need to recognize the impracticability in the IOT universe of transparency and control of giving any real control.

I mean, to Chairman Wicker's point in his opening statement is that really a choice. And I'm wondering Mr. Steyer and then Ms. Guliani. How much of this do you think can be accomplished to transparency and control? How much of this do you think ought to be back up...

WICKER: Yeah.

SCHATZ: ... with the principle of, listen, we're going to configure a statute best as we can. But in order of the future proof this and in order to back this thing up, we have to have a basic principle in the law which says, you may not harm people with the data that you collect.

Mr. Steyer?

STEYER: I completely agree with you. You can read my remarks. I agree with the transparency and control are important but they're simply not enough themselves. And we talk about the rights to access, to delete, to put your information in certain limits that should be completely off limits like the behavioral ads targeting kids.

So, transparency and control are good but they are simply not enough. Notice and consent sort of broad term like that just are not enough. We have to go further and we think that on a bipartisan basis the public would love you to do that.

SCHATZ: Ms. Guliani?

GULIANI: Yeah, I think you're absolutely right. Notice and consent aren't enough in part because in a lot of cases people don't have multiple choices.

WICKER: Right.

GULIANI: Right. If the option is between not having a service at all, we're turning over, you know, massive amounts of data. A lot of consumers, you know, consent but it's not really consent. So, I think that the law should play strict guardrails on what companies can and can't do.

For example, you know, if I have a flashlight app and is it really reasonable for the app to require me to turn over all of my location data or my financial data just as a condition of using that app. I would say no.

And in the face recognition context, you know, if I want to go to the grocery store to buy food, is it really reasonable that the only option I had was the sign that notifies me that this recognition technology is being used? I don't think that's really the control and the right the consumer wants.

And so, absolutely, we have to go beyond notice and consent to get that sort of terms that or really take advantage of people's privacy and exploit their lack their choice.

SCHATZ: My final question and this would be for the record and for the entire panel is whether or not we are missing anything in terms of essential elements of a federal data privacy law. And I'll take that for the record. Thank you.

WICKER: That's a very good question. And so I'd hope all of our panelists will take that for the record and you have a few days to respond, that would be very helpful.

Senator Fischer?

FISCHER: Thank you Mr. Chairman. One core part of the GDPR is to protect consumer data by requiring freely given, specific and informed consent, however we already are seeing user interface work around that we can consent by confusing use of choice.

Ms. Guliani -- Guliani, you just spoke to that and answered to Senator Schatz's question. In these circumstances users see a false choice or a simple escape route through the I agree button or OK button that pops up on our screen. And this can hide what the action actually dose, such as accessing you contacts, your messages, web activity or location. Users searching for the privacy friendly option if it exists there at all often must click through a much longer process in many screens.

Mr. Steyer is clear easy to understand user interface design a critical component of achieving informed consent and preserving any rights to consumer data privacy?

STEYER: That's a great question Senator Fischer and it is, it really is. I think the truth is if we all think about ourselves, maybe there's one or two wizards up here but I'm not and I run a large organization that helps write privacy laws. So, I think clear, easy to use information is absolutely critical. That's why I mentioned it in my opening remarks that consumers just need -- is this the complex stuff.

And -- so we need to make it very easy for consumers to understand what their rights are and then how to exercise them. It's unlike having a privacy policy at the end of your phone, 80 pages on your phone which no one ever reads, they just check here.

So, I think that's a really important element of what this committee and the Senate could do is, make it simple and easy to understand for the consumer, if it's easy to understand for you folks it will be pretty-- it will be fair to the consumer, that would be what I would say.

FISCHER: I hope that's an endorsement.

STEYER: That's an endorsement, it's an endorsement, but it's also a recognizing the complexity of this...

FISCHER: Sure.

STEYER: ... that actually goes you know, question Senator Schatz was asking too. But it's really an important element of doing this right.

FISCHER: Right. I appreciated Common Sense Media Endorsement Bill that I have with Senator Warner, the Detour Act.

STEYER: Right.

FISCHER: And I believe that's going to guard against the manipulative user interfaces that are out there, those are also known as dark patterns.

STEYER: Right.

FISCHER: Can a privacy framework that involves consent function properly if it does not also ensure that user interface design presents that fair and transparent options to manage our personal data settings are?

STEYER: Is that indirect (ph)?

FISCHER: Yes.

STEYER: Yes, you're absolutely right on that. By the way the other point I would make is the fact that you and Senator Warner are working on the dark pattern, the fact that Senator Blunt is working with Senator Markey and others, I'm bipart of one second (ph), this is an area where I keep saying it. This is common sense for everybody and I really do believe that this committee acting this way in a bipartisan fashion is critical.

But yeah we got to keep it simple and easy even though its complex, you've got to make it simple and easy for the average user.

FISCHER: Thank you.

Ms. Dixon, as the GDPR has been implemented have you seen any trends for companies that have taken steps toward focusing on user centered design or others that are avoiding it on purpose?

DIXON: We certainly -- in the run up to the GDPR saw a lot of attempts in particular by the platforms to redesign their user engagement flow and to reexamine whether the consents they were collecting met the threshold articulated in the GDPR, but some of the investigations that we now have underway are looking at whether the ways in which in particular the transparent information is being delivered to users really meets the standards anticipated by the GDPR.

So, for example a lot of organizations have implemented layered privacy notices which is something generally that we recommend to avoid the need to have a 100 page privacy notice. But on the other hand there can be issues of inconsistency between the layers, too many layers for a user to go through to get basic information.

So, through the investigations that we have on going at the moment we're examining whether the standards anticipated by the GDPR are being met (ph) and in what circumstances we say they are not being met, so there should be further clarification on that in the coming months.

FISCHER: So, as Mr. Steyer was saying keep it simple.

DIXON: Keeping it simple is always good.

FISCHER: And so we look to draft federal data privacy policy it is important that we do look at preventing an irresponsible data use from the start, Ms. Dixon you actually noted the complaint of someone who had been contacted by a headstone company after a family member passed away generated by combining obituary data and public address data, and I'm going to ask all of you the same question that I asked the previous industry panel and hopefully you can respond in writing to the questions since I'm out of time.

But I was -- I would just really appreciate if you could give one example of an unreasonable data practice to us. I think that would be helpful when we do look at trying to keep this simple and what's going to be needed. So, thank you very much. Thank you Mr. Chairman.

WICKER: Can each of you do that for us on the record? We would appreciate if you would.

Senator Tester?

TESTER: Thank you Mr. Chairman, thank you all for being here. I know you all came to talk about production and today.

So, I'm going to ask some questions about it. I've been farming for about the last 40 years and one of the big advances in agriculture has happened pretty recently it's called precisioning where you get computers on your tractor that measure just about everything you do, from the amount of fertilizer you put down, to the kind of seed you put in the ground, and the number of acres you've covered, you name it.

So, I've got this information as obviously connected up with a higher God. Is it possible for folks or, you know, if they can use that information right now, if they can gather that information to try to influence my marketing, my buying decisions?

You understand what I'm saying? I'm saying we've got technology on the tractor that measures just about everything you do. Is that information gatherable? Is somebody taking that information sweeping it up is it possible for them to do it? Can anybody answer that?

GULIANI: So, I can -- I answer specifically I think with the agriculture and some of I think the new technologies, I do think that a big problem is secondary uses, right? Think about if I buy, you know, eggs from a grocery store...

TESTER: Yeah.

GULIANI: ... and I give somebody my address to deliver those eggs.

TESTER: Right.

GULIANI: I expect that they're going to use my address to get the eggs to me, what I don't expect is that they're going to tell an insurance company that I bought eggs...

TESTER: That's right.

GULIANI: ... and that they should charge me higher rates.

TESTER: OK. So, what gives them the right to do that? What gives them the right to share that information? It looks to me like why should not all be off the books unless I say, you know, what, go ahead give it to my document, give it to my insurance company, give it to the guy I'm going to buy a car from, I don't care go ahead and do it. Otherwise if I don't do that, no sharing information, period. What I do is my business and nobody can share it, it's against the law.

GULIANI: I mean I would agree and I think that what functionally happens sometimes is that there is a 30 page privacy policy. Somebody doesn't understand what's in it nor do they have the time to read it

TESTER: So, it looks to me like it doesn't have to be 30 pages doesn't? Could have been just a simple question, can we use your information yes or no?

GULIANI: Yes. And I don't believe that there should be secondary uses and secondary sharing unless the person knows what's happening and has provided specific consent for it.

TESTER: OK. So, the lady from Dublin, would the GDPR stop the collection that I just talked about? And by the way this is a scenario I use for agriculture, but you can use it on anything. Would they stop it? Would your role stop it?

DIXON: Thank you Senator. It's a very interesting question. As I mentioned in my written statement the GDPR is high level principles based technology and neutral and it doesn't prohibit any specific forms of personal data processing, it provides that any form of personal data processing could be legitimized.

So, in this case what we would have to do is trace through the various actions of the company and look at whether the principles of the GDPR are being measured particularly in this case around purpose limitation, transparency to you as a user in terms of the sharing the data with third-parties.

TESTER: Yeah.

DIXON: And the purposes for which it would be used. And today extends that consent is legitimizing the processing, whether you would grant either option is to consent or not to consent. And, so it is possible that the GDPR would prohibited depending on how it's being done.

TESTER: OK.

DIXON: But with involves specific...

TESTER: It can be.

DIXON: ... tracing against the principles.

TESTER: The previous question I asked you about fines and you said none of them level yet, because in these investigations haven't been done. What -- and what's your longest, given effect for 11 months, since we have put into effect?

DIXON: Its 11 months since the GDPR came into application...

TESTER: I know.

DIXON: ... some of the investigations have been open more recently, but we have one or two their options...

TESTER: What's in...

DIXON: ... and since the May.

TESTER: Since May, (inaudible) for the investigations?

DIXON: That's right.

TESTER: How, quickly are they to the point where you can -- are these investigations were complicated or they going to look another year or is it we use...

DIXON: No, and I think in the coming months over the summer, enabling conclude decisions and some of them they are a complex investigations. The road so significant to procedure and safeguards that we have to apply, because the sanctions are significant, so we do have to allow the parties is right to be heard at various junctions in the investigation and decision-making. In addition -- because of...

TESTER: Are the...

DIXON: ... the form of one stop shop, we haven't in the EU and other procedure issues it was.

TESTER: OK. And very quickly, because my time has run out. How are the fines level it, how do you determine the fines? Is that dictated in the GDPR or do you do it on the size of the company? And what and how do you that?

DIXON: So, Article 83 of the GDPR set size at the limits on the fines and provides details of aggravating and...

TESTER: Can you give me an idea of what the largest fines are on your computer?

DIXON: The largest fine it would be 40% of the global turn over for the preceding year of the undertaking.

TESTER: OK, thank you.

DIXON: Thank you.

WICKER: Thank you Senator Tester.

Senator Blackburn?

BLACKBURN: Thank you, Mr. Chairman and thank you to each of you for being here today, and Mr. Steyer, good to see you.

STEYER: Nice to see you.

BLACKBURN: We've been talking privacy for a quite of while.

STEYER: We have.

BLACKBURN: And I -- and, you know, as Ms. Guliani, I'm certain you know this and to our friends who have joined us today. I think that for so long what we heard on the Capitol Hill from the people is don't do anything that is going to harm the golden goose. Leave it alone. And this is why I introduced the BROWSER Acts several years ago, bipartisan in the House. And why I have long held that consumers need to possess the toolbox to protect this.

I term it the virtual you, which is you and your presence on line. And this is vitally important as Americans moved more of their transactional life online. And Ms. Guliani you said it well, there should not be a secondary use for other companies to know what credit cards we use, what time and month we have pay our bills. Besides we search the products we order and for that to be data mined. And then repackage and so specific not to our name our physical address maybe. But to our IP address. Which is our virtual you (ph).

And so, that is one the BROWSER -- it does a few things very well. It says opt in for a sensitive data, opt out for non-sensitive data. And one set of rules for the entire Internet ecosystem with one regulator.

And I think when we looked at in individuals privacy that we ought to focus, on doing a few things well. To do it understandably. And as we have discussed in past Mr. Steyer, that make certain that the protections are there for children. And that their information is protected online.

And so, is -- and I'm delighted that the Chairman is bringing this issue forward privacy and data security are essential. And because, this transactional life that we live online, underpins every single industrial sector of our nations economy.

And Ms. Dixon, I want to ask you about the difference, let's say for Ireland having an EU wide regime on privacy is supposed to an Ireland specific? Preemption I think is vitally important. And I would like to hear from you what the difference has been by having the ability to have it EU wide versus just for Ireland?

DIXON: So, Senator Blackburn, the GDPR as you know, has a direct effect to regulation of the EU as opposed to a directive, which requires transposition into member state law, which was the previous regime we have prior to last May.

But, in fact, as a regulation the GDPR is still something of a hybrid, because each EU members state nonetheless, has it -- had to implement to national law to give further effect to the GDPR. And because, in fact...

BLACKBURN: It underpins it, correctly? It underpins.

DIXON: It underpins and...

BLACKBURN: Correct.

DIXON: ... gives further effect to the GDPR and implements some choices that were left to each individual members states on the GDPR. So, what we have is actually a hybrid, where we have a 2018 Irish Data Protection Act that guides us in terms of the operation of our investigations and the procedures. We must follow and to run the aspects, such as the age of digital consent for a children which is set at 16 in Ireland. And then we have the GDPR.

In the case of any conflict, which there shouldn't be the GDPR reigns supreme under the doctrine of supremacy of EU law. So, it is something of a hybrid and there are still a member state flavors in the terms of choices made them to the GDPR.

BLACKBURN: Thank you.

I appreciated a visit with your EU Privacy Commissioner a few weeks ago. And then this week, visited with the commissioner from New Zealand. And I think it's an instructive to us in that whether it is -- GDPR if (ph) it comes through it's the first year of enactment. Or other countries that are looking at an acting privacy policy, the data is important to our citizens that we do something and that we do it right the first time.

So, I appreciate your participation. I look forward to continuing the conversation. I yield back my time.

WICKER: Ms. Dixon, the GDPR directs member -- European member states to make certain decisions, for example the age of consent, is that what you're saying?

DIXON: So, under certain articles of the GDPR such as Article 8, the age of consent for the children accessing information, society services, was set at 16. But it gave member states the choice to implement as low as 13 under their member state laws. So, in fact, which you find is that the majority of EU member states went ahead and implemented an age of 13.

So, there are a number of articles like that for a member state choice, was...

WICKER: OK. Well the -- and maybe we could search that ourselves, but if you would help us by supplementing your testimony and giving us some examples of that, I would appreciate it. Thank you.

Senator Peters?

PETERS: Thank you Mr. Chairman, and thank you to each of our witnesses it have been a -- really a fascinating discussion.

And Mr. Steyer, I do believe you're right. So, that this is report issue that until the time is now. In fact, I think this is the issue of privacy given the explosion of data and technologies with the power to collect a lot of data are continuing to expand.

This could be the one of the defining issues of this decade, as to how we deal with that, because with data comes power and that power is based on the data collective from us and each individually. So, we have to be leading (ph) into those very heavily. So, I agree with that.

My question -- first question though for you, Ms. Guliani is that -- is the example of some concerns that I have. There is a popular a pregnancy tracking app Ovia that tracks medications, mood, bodily functions and more. And that even use how to track newborn medical information from women that used this app, you maybe familiar with that.

The app is come under scrutiny because it allows the employers to actually pay, it's a gaining access to the details about their workers personal lives. Your testimony and you were very clear and others have mentioned about how federal should limit the purposes for which consumer data can be used.

So, my question now is what should be included in the federal privacy standard to ensure that employers in particular cannot have access to their employee's medical information from an app such as Ovia?

GULIANI: I mean I would say first that that is information that shouldn't be given to an employer absent the consent of the individual using the app. And they shouldn't be denied using it, if they say, look I don't want my employer to know that, but I would still like you to measure these things.

So, I think that those are sort of two sides of the same coin. And what I worry with apps like these is again this long privacy policies that individuals don't have time to read or understand that effectively require them to sign away all these rights, just to use the service.

PETERS: Well, to follow up on that comment. In Ovia, they have a 6,000 word consent form. The company has granted, "A royalty-free, perpetual, and irrevocable license, throughout the universe to utilize and exploit their de-identified personal information. The company is allowed to sell lease or lend aggregated personal information to third-parties." This basically means that all of the information that's gathered, a package can be sold to who ever they want, whenever as long as it doesn't meet their de-identified criteria.

But how difficult it is for a company to re-identify someone if there is enough data about them, let's say a smaller company that may only have one woman who is pregnant, could you identify that person probably even with the de-identified data?

GULIANI: Yes, I mean, re-identification, I think is becoming easier and there are companies that are innovating around that. So, for example there have been MIT studies that found that de-identified data could be re-identified 95 percent of the time with accuracy.

So, I think it's really important that when we talk about the de-identified data we're really clear on what that means and making sure that it is in fact de-identified.

PETERS: Right, right.

Mr. Polonetsky, for example, if I go to the doctor and I get prescribed an allergy medicine and then I put that information on my -- on an app that I have to keep track of the number of doses I have to take medicine or whatever it maybe. How do you envision a federal privacy law working with existing law such as HIPAA to ensure that my medical information is indeed protected after I put it on my own app?

POLONETSKY: Yes, this is increasingly going to be an important issue because patients are increasingly downloading their medical records. And there's obviously great value when people be able to see that data, maybe take it to a different doctor, analyze it themselves. But they may not appreciate that once they've downloaded it from their HIPAA Covered Entity that it is now in their hands, it's in their app.

Legislation should recognize that there are sensitive categories of data that are going to be subject to much stricter and tougher controls. I may want to share that with another doctor. I may have a friend who was a doctor. I may want to show it to my spouse, and so I certainly should be able to share it, but it ought to be very clear and very practical. And I would be able to revoke that consent.

It isn't likely to be covered by HIPAA, but we increasingly have data that is outside of the regulatory world where we need to make sure that the consent standard in any proposed legislation is indeed balanced.

PETERS: Yes, in March, it was reported that a data broker tried to sell the names, addresses, high schools, and hobbies of 1.2 million children. This was uncovered through the violation of Vermont's recently enacted law to regulate data brokers.

Mr. Polonetsky, as you know, the Vermont law requires data brokers to register with the state annually and gives us some transparency as to who's actually out there, who's actually collecting all this information.

Understanding with the law was just recently implemented, you have an early assessment of the law and should we look at that law in guiding some of our work at the federal level?

POLONETSKY: Yeah, I don't have enough information to know how it is playing out, but it's clear that people today have limited idea of the number of places their data goes when they're online or when they can transact in providing a simpler way for them to get to those end points so that they don't go to multiple places.

So, they can say no ones -- so they can go to one place and effectively take their data out I think is valuable. Frankly, I think it's valuable for companies too, the people who really don't want to be getting catalogs in the mail, don't want to be marketed too, it's costly to send some of that out.

And I'd like to believe that at the end of the day there's a win-win by giving people more control over what they receive from a whole range of third-parties.

PETERS: Thank you. I appreciate it.

WICKER: I think there are a lot of win-wins out there.

Senator Thune?

THUNE: Thank you, Mr. Chairman.

Ms. Dixon in your testimony you touched on industry codes of conduct. Can you elaborate on how industry codes of conduct are intended to operate under the GDPR? And whether you think such codes of conduct enhance compliance with the law?

DIXON: So, codes of conduct are new feature EU Data Protection and we do believe that they're going to pay dividends once they get off the grounds.

The European Data Protection Board has recently issued guidelines on how it's intended the codes of conduct would work. And in the first instance it's up to industry grouping to bring forward proposed codes of conduct that they would agree to implement. They have the benefits of creating a level of playing field within industry sectors and driving up standards.

Another key feature of codes of conduct under the GDPRs that it's intended that there would be an independent monitoring body paid for by the industry sector that would monitor compliance with the code of conduct and ensure that complains from individuals that the exercise of their rights for example isn't being adhered to our judge (ph) efficiently. So, this is an area of the GDPR that we look forward to ruling out over the coming years.

THUNE: OK.

Let me just direct this to everybody, and so it's more of a general question, but Mr. Polonetsky, Mr. Steyer, and Ms. GULIANI, with respect to privacy expectations for consumers here in United States, do you think the status quo is working, yes or no?

STEYER: No. But I would tell you that there's been change in awareness last year. I think one of the most encouraging things that we've seen other than the bipartisanship, I think in understanding these issues that affect everybody is that the public is finally coming to understand that privacy really matter.

Remember, it's a fundamental right, but people have forgotten that. And my -- I have four kids and I remember talking to my kids about this a few years ago about, do you even respect -- do you even understand what privacy is?

So, I think we're the watershed moment which I think the work of this committee and the broader Senate and Congress will drive forward. That the public is finally saying, this is really my own personal information, it's really important and I have the right to control it.

So, I think where the great moment, I think that, honestly Senator Thune, if this committee moves forward and the Senate moves forward I think it will be incredibly important not just legally and from an enforcement and accountability standard on for the behavior, but public awareness.

THUNE: OK.

STEYER: So, I think where the really important tipping point that you all can drive forward in a very important way.

POLONETSKY: Yeah. Senator, my 17-year-old son is sitting behind me and I've got a 15-year-old daughter and it's been fascinating to see how they had been using technology, and I don't think they think about it in terms of privacy. All they know is that their Instagram page shouldn't have all of their photos, it should have the ones they curate. And they may have another account that they use a little more flexibly, a little more sloppily.

My son is a big Snapchat user and he's not thinking about it, oh, my pictures disappear. He just -- I'm just saying, hi, why should that be around forever? And so, optimistic that the technology is finally capturing the actual reality of how people act. Somehow when some of these sites launched, the notion was, the more you share, the more people click on it, the more people see your stuff, and there's a place for that, for activism, for outreach, but that's not the default for the way most of us live. We want to talk to friends and family and small groups and alumni groups and the like. And somehow the engineering answer was, sorry, if it's on the Internet and it's public, it's public for everybody.

So, these aren't perfect, you know, it's not perfect privacy when your photo disappears, it's possibly somewhere. But it gave me a level of obscurity that actually ends up being critical and nuance. So, I'd like to see as nudge companies to solve some of these problems by having technology reflect the way humans act, right? It's supposed to be in service of our needs...

THUNE: Yes.

POLONETSKY: ... not in service solely of advertising in marketing. I see that pushback happening. I'd like to think it's because of privacy pressure, but I actually think it's because of what the younger generation actually wants. And they don't call it privacy, they call it, this isn't the way I think about my relationships.

THUNE: But the answer is no, status quo is not working.

POLONETSKY: The status quo is not working, but...

THUNE: And Ms. Guliani, yes or no, could -- and I had another question I need to ask you but...

GULIANI: Yes. The status quo was not working. And I just want to highlight, I think that we're increasingly understanding that, that status quo is hurting vulnerable populations in some cases the most. You know, exacerbating and economic inequality in some of those issues. And so I think the law should reflect the special harm that's being placed on consumers.

THUNE: And I agree the status quo is not working which is exactly why this committee begun to lay the ground work for privacy legislation, in the Congress weren't billing on that. I believe it's one of the issues that Congress should be able to work on together on a bipartisan basis and I look forward working with Chairman Whicker and all the members of this committee to find consensus on this very important issue.

One very quick final question and, that again, it can be yes or no, but on principle with any of you oppose any federal law with preemption in it, yes or no?

GULIANI: We would have serious concerns with broad federal preemption.

STEYER: I have serious concern with broad federal preemption.

THUNE: OK.

POLONETSKY: I think preemption can be done carefully so that it preempts the inconsistencies that make compliance hard but preserve the rights and protections that I think we want to preserve.

THUNE: OK. I would be interested and I guess we can take this for the record, Mr. Chairman, but in your thoughts, you all referred to a federal law as strong as California. And just maybe speak specifically to what you mean by that.

Thank you.

WICKER: Thank you.

And Senator Thune you questioned long enough for Senator Markey, so get back in your seat.

Senator Markey is next.

MARKEY: Thank you, Mr. Chairman very much and thank you Mr. Thune -- thank you Senator Thune.

I've long advocated for privacy protections that include the principles of notice and consent, but a federal privacy bill must built on that framework by explicitly prohibiting certain types of data use.

Today, companies are must throws of consumer's data and then repurpose that information to target ads in discriminatory ways. And that is why I recently introduced the Privacy Bill of Rights Act, comprehensive privacy legislation that bans discriminatory uses of consumer's private information.

This legislation explicitly prohibits companies from using Americans' data to target employment, housing, health care, education or financial opportunities in harmful discriminatory ways.

Ms. Guliani, can you provide one example of how a company currently uses consumer's personal data to target individuals, particularly genders or socioeconomic groups in ways that threaten American civil rights?

GULIANI: Sure. I mean I can give you a recent settlement in an ACLU case. You know, over the last several years, there were multiple charges that Facebook was facilitating discriminatory advertising, particularly in the housing credit and employment contacts where federal law prohibits discrimination.

So, for example, allowing targeting of ads based on, you know, factors like race or gender or things that would be proxies for that. Over the years, complaints were made. The company said that they were going to resolve the problem, but were supposed to do so. And so the ACLU and other civil organization -- civil rights organizations files lawsuit and the company to his credit has settled that lawsuit.

But I think what this does is speak to, you know, a broader concern and that's a question of how in this online -- new online ecosystem are advertisers and others exacerbating discrimination, charging different prices for let's say a bus ticket, not allowing African-Americans women to see employment or housing opportunities.

MARKEY: OK.

So, let me just follow up in that, do each of the rest of you agree with Ms. Guliani that it should be illegal for companies to use consumer's personal data in this harmful discriminatory ways?

Ms. Dixon?

DIXON: So, Senator Markey, I think in terms of legislation prohibiting certain uses as I've outlined, the GDPR set up as principles based and doesn't specifically prohibit uses but principles of fair processing as an example will go some way to tackling the issues that you've outlined. I think in terms of the issue of discrimination, and there are some complexity to the issue and...

MARKEY: But in general, do you agree with Ms. Guliani, in general on discrimination?

DIXON: In general discrimination, right.

MARKEY: OK, Mr. Polonetsky?

POLONETSKY: In general, yes.

MARKEY: OK, in general.

Mr. Steyer?

STEYER: Absolutely I agree with Ms. Guliani.

MARKEY: Now, thank you all.

So, let's move to children's privacy. I'll go to you Mr. Steyer. Children are a unique vulnerable group online that's why earlier this Congress introduced bipartisan legislation with Senator Hawley to protect kids and teens privacy. This legislation is an update to the Children's Online Privacy Protection Act, the law which I authored back in 1997.

This law creates critical new safeguards for young people. The legislation would extend protections to 13, 14 and 15-year olds by requiring consent before collecting personal information about them, ban targeted ads to children, create and erase a button for parents and children to allow them to eliminate publicly available personal information submitted by the child or teen and establish a youth privacy, a marketing division at the Federal Trade Commission, which will be responsible specifically addressing the privacy of children and minors in our country and marketing directly at children and minors in our country.

We know we have a crisis in the country in terms of the targeting of children in our country by all -- by these online companies. So, Mr. Steyer, why is it critical that any comprehensive privacy law include this heighten protections for children and teens?

STEYER: Well, we totally support the law and we're glad it's bipartisan and you have Senator Hawley on it. Look, we just believe you should fold the COPPA 2.0 law into this broader law that you're doing.

The truth is, we all know this as parents and grandparents, kids don't understand stuff. They may be more technically literate in a way, but they just don't understand it. So, they deserve special protections and the COPPA 2.0 law that you all have introduced is absolutely spot on and I would urge everybody on this committee and all 100 senators to support it.

MARKEY: Do you each agree that special protections have to be built in for children? Ms. Guliani?

GULIANI: Yes.

STEYER: Yup, yes.

MARKEY: Mr. Polonetsky?

POLONETSKY: Yes.

DIXON: Ms. Dixon?

DIXON: Yes.

STEYER: And teens...

MARKEY: And teens.

STEYER: The (inaudible) with COPPA is it stops at 12.

MARKEY: Yeah.

STEYER: And you really -- we all know what teenagers are like. They need protect -- special protections too.

MARKEY: So, this bill would lift up to 16.

STEYER: Correct

MARKEY: And that's kind of I think a reasonable place to put it. I wish I could make it higher, but I think at least at 16 kids are just unaware, even though what you're saying, technically sophisticated what their judgment in terms of what they might mean -- what it might mean for themselves in the long run just hasn't been well (inaudible).

STEYER: And California goes to 16. We took it up to 16 in the CCPA.

MARKEY: And in Europe?

DIXON: Sixteen in Ireland, 13 in other member states.

MARKEY: Yeah. I like -- I'm Irish, OK, so we like our privacy, you know. Thank you, Mr. Chairman.

WICKER: Thank you, Senator Markey.

Senator Moran?

MORAN: Chairman, thank you. Thank you four for joining us today on this important topic. Let me start with Mr. Polonetsky. The term -- terms of federal consumer privacy bill, consumers I believe would benefit if Congress provides clear and measurable requirements in the statutory text while also including level of flexibility in the form of narrow and specific rule making authorities, presumably to the FTC. That would help account for evolving technological developments.

My questions are, how should this committee approach providing FTC with rule making authority? And do you see value in what some of us have been calling strong guard rails around that rule making authority to preserve certainty to consumers that we aimed to protect?

POLONETSKY: I think our proposed legislation, the committee's proposed legislation, which hopefully will come forward, should put as much detail as we can put in the bill because I think there are going to be key issues to negotiate.

But clearly, there are going to be areas that are going to need more time where progress of time is going to require perhaps updates and nuance and the FTC certainly needs APA rulemaking authority to fill those gaps.

But I do think setting the parameters so that the considerations that the FTC should look at can be spelled out so that businesses can anticipate so that the commission heads no matter what party is in leading and so forth in the right direction I think is going to be critical.

MORAN: This isn't the -- exactly the right words, I don't think, but the theory that I have is that we have to provide lots of certainty but not too much certainty, just -- where do we find that sweet spot that allows us to work well today and into the future.

(OFF-MIKE)

MORAN: Thank you.

Ms. Dixon, you indicated in your testimony -- I'm think I'm quoting this about right, the aim equally of a consistent and harmonized data protection law across the EU is to ensure a level-playing field for all businesses and a consistent digital market in which consumers can have trust.

Would you have -- let met ask it this way. Would you be concerned that EU consumers trust in the digital market would be undermined if the EU lacked a harmonized approached to privacy? And related to that is do you think the GDPR has provided clear privacy requirements to companies that if each EU country adopted a different privacy requirement?

DIXON: So, I think certainty would be the case as EU service users trust would be undermined if we don't give full effect to this harmonized regulation now in the EU and in more case of companies rather than consumers at the moment arguing that some of the harmonization is not coming into effect as anticipated because of member state choices that have been made.

So, the European Data Protection Board is a grouping of all of the EU National Supervisory Authorities and we're working very hard to give effect to a harmonized implementation through guidance that we issue, but also through a cooperation and consistency mechanisms that Neema and I conclude the investigations I referenced earlier.

I will have to bring my decision to the European Data Protection Board and take utmost kind of the views of the other EU 27 in finalizing my decision. And so I think the harmonization is extremely important, not just in terms of the level playing field, but it terms of the consumer trust.

MORAN: Thank you. A question that -- I mean, part of the conversation here has been things are getting better, people are more interested in privacy, but we've also talked about how difficult it is and what you're thinking about when you opt-in and opt-out where the responsibility lies.

Are consumers currently considering privacy practices when choosing between an online service provider? Are there enough companies using privacy as a competitive advantage? Anybody -- any consumer like paying attention to this and there's now an economic reward for privacy protections?

STEYER: I'd like to speak with that. I think -- look, when we passed the California bill last year, we were working with Satya Nadella, Tim Cook -- Satya at Microsoft, Tim Cook at Apple, Marc Benioff at Salesforce. They absolutely know that that -- there's no way Apple and Microsoft don't see that as a competitive advantage now which Senator Moran, I think is a very healthy thing.

But that alone is not enough. I mean you still need, that's why I said in my earlier comments about how important it is for the Senate and for the Congress to pass comprehensive strong federal privacy protections.

But there is no question, just look at Apple's marketing campaign that's out there right now. They're all over privacy. We meet with the -- at the top levels all the time. They have decided this is both the right thing to do and also the right thing to do for their business. And so it Microsoft so the wave is coming.

MORAN: What a great blend that would be if we do our jobs correctly and the consumer demands this from their providers.

STEYER: Agreed.

MORAN: Let me ask a final question just a yes or no answer, if Congress were to enact this what we hope is meaningful privacy legislation would you each support the attorney general of our various states having enforcement capabilities?

GULIANI: Yes, I would strongly encourage that as well as state enforcement agencies.

STEYER: Completely agree, absolutely I think state AGs are critical and a private right of action is a good idea too.

POLONETSKY: AGs have a key role.

MORAN: Thank you all very much.

Thank you Mr. Chairman.

WICKER: Thank you.

Senator Rosen?

ROSEN: Thank you this is an amazing hearing and I have so many questions. I'm going to first start with some vulnerable population questions. One of our most vulnerable populations our seniors, our disabled veterans, our hearing, our deaf community.

I have over 38,000 deaf and hard of hearing people in the state of Nevada, the rely on IP caption telephone service to communicate, we all know what that is and so, what are the privacy concerns, what are we doing to protect those vulnerable populations who are using the telephone, using these other services because of a disability?

GULIANI: So, I think that this is one of the reasons that having a privacy framework is so important, I mean you mentioned the disabled population, low income individuals rely on their phones more for Internet access and to do other day-to-day activities. And what we don't want is a system where as a condition of using these things that are critical to everyday living people have to hand over their personal data and that personal data can have downstream consequences.

And so I think that as part of, you know, any framework we have to consider number one limiting the extent to which somebody can require you to give consent just as a condition of using a service. And we also have to be really skeptical in that law, sort of what's been called pay for privacy schemes, where I'm just going to charge you more if you choose exert your privacy rights.

POLONETSKY: Senator I urge the committee from the disability community because I think there is actually a really nuanced set of use, certainly the community -- and I won't speak for them, although we've done some joint work recently, is worried about new ways that they can be discriminated against.

But they are also passionate about the ways the assisted technology and data -- they want a smart home speaker to be able to control devices if they can't use a traditional UI. They don't want the data sold. But getting that balance right, so the data that you do want can support them is certainly important.

ROSEN: So, as I've been sitting here listening and I get the pleasure of being one of the last questioners is that it seems to me that there's two issues about your data, it's time for who, what, where, when and how. The who is your personal data, it's your name, your birthday, your social security number, whatever you own that right, your baseline definition.

Then you have your recorded behavior if you will, your usage, your active usage, your passive usage, what's caught on recording on geolocation that's your what, when and how.

So, the real issue is who owns your behavior, right? That's what the -- I mean the new safety issues security for your personal birthday and all those kinds of things. But -- so owns your behavior is the issue and what do they do with it and the real value and the real threat is the monetization of you usage data.

That's where it is, it's the economics, let's just put it right there. So, how do you think that we can tailor some legislation that protects your usage information? We're trying to get better by protecting that personal identity the who but what about the what, where, when and how that happens outside of you, where you shop, where you drive by, where you record on your voicemail?

POLONETSKY: So, Senator Rosen, I mean it's a very important question, it's a very good question. I think the truth is we should probably protect -- allow the individual to control their own, not just their data, but their behavior.

And therefore I use the term earlier data minimization, it was one of the big issues, in the California law and in GDPR which is you should only be able -- a company should only be able to use the data for a necessary business purpose not a secondary purpose.

When Senator Tester was asking the question about the farm implements, how -- why should that be so...

ROSEN: Or the pregnancy.

STEYER: Right, or the pregnancy.

ROSEN: Same thing.

STEYER: So, I think a very strict and clear limits and guard rail around that is absolutely critical to a strong privacy law. I think everybody on both sides would agree with that. And again, the more you guys can make that clear to your colleague but also to the public, the more we will all win.

ROSEN: And what do you think, since there's such a strong economic benefit toward the monetizing of your data...

STEYER: Yeah.

ROSEN: That should be strong economic sanctions if the violations occur?

STEYER: I would and the only thing I would just say is the big that simplify it is the business model, is everything. So, if you really want to understand how the companies behave, because remember the technology industry is monolithic.

You really have to take them company-by-company. It's all about the business model. So, if their business model is based on monetizing your personal information through ads, you are going to have to restrict those companies much more. It's that simple.

ROSEN: But what about using new technology. So, you have a smart car. You're going to drive by a certain coffee shop or grocery store everyday. Do they say well this person drives by there, your -- that's a kind of your location, it's your passive usage?

STEYER: If I opt-in. If I opt-in to that like give the consumer the right to opt-in, not force them to opt-down.

ROSEN: Right. Thank you appreciate, I yield back my time.

WICKER: Thank you very much.

Senator Blumenthal?

BLUMENTHAL: Thank you Mr. Chairman and thank you for having this hearing with this very expert and knowledgeable witnesses. I have heard a lot of worries about the ongoing effort and I'm a part of it in the Congress to frame Federal Standards that will protect privacy.

I've asked one panel out for another whether the people of the United States should have less privacy protection in California. Nobody believes they should. And I assumed nobody on this panel thinks that the people of the United States deserve less privacy protection than the people of California, correct?

STEYER: Correct.

POLONETSKY: Correct.

BLUMENTHAL: Thank you.

At the same time, there is a legitimate fear that we would either advertently or maybe inadvertently undermine state protections. I think that's the real danger. And I would oppose any effort that preempts state laws so as to weaken protection for consumers. And I think we are all or we should be on guard against that danger.

I know that business is what a common definition and consistent rules. I also understand some of the criticism of the California law, some of that criticism smack of opposition to the protections in the substance of those safe guards for consumer protection.

Federal rules simply cannot be an opportunity to weaken a strong framework that industry resists or opposes. We can learn from California. We have to provide at least the same standards. In fact, I believe they ought to be even more rigorous and more protective.

So, let me ask particularly Mr. Steyer and Ms. Guliani, if Congress fails to act now, are other states likely to successfully pass similar bills in the near term? What is on that horizon?

STEYER: So, I can speak to that and I'd be happy to. And I would say, you know, the state I believe Senator Cantwell knows, the State of Washington just considered a fairly -- it's -- it was different version of the bill and it died in there.

It's the only one that's on the table right now. So, the boring action by the Congress, the California law goes into effect in January 2020 will essentially become law of the land. And I believe that the Tech companies understand that.

And we -- when we were writing it, we were aware of that. I don't think you're going to see this hard parts (ph) mishmash. And to your point Senator Blumenthal, the people who are really raising the -- pushing preemption are primarily certain tech companies that want to weaken the California law.

So, your point of view about that is a floor that we should build upon for a strong comprehensive federal law is I think a very good framework.

BLUMENTHAL: A floor, not a ceiling?

STEYER: It's absolutely a floor and not a ceiling. And I think there are some very smart folks on this committee who can...

BLUMENTHAL: Who can first...

STEYER: ... and even better law.

BLUMENTHAL: ... first to no harm.

STEYER: Exactly.

GULIANI: And if I could just speak to that point specifically. I mean I think particularly in the area of technology, we're talking about rapid changes. And states have shown themselves to be more nimble and adapt to responding to those rapid changes.

So, what I really fair is a federal regime that ties states hands and when new technologies pop up, new problems pop up, we see gaps in the federal framework that they're not able to -- they're not able to address those problems. And I think particularly in area where when it comes to consumer rights and consumer privacy, states have a long history of expertise and a long history of leading on these issues.

BLUMENTHAL: Well I share your prelections about the important of state action having been a state official for about three decades and including two decades as state attorney general in Connecticut. And both in terms of being more nimble and also closer to their constituents and sharing the effects, we share the real life effects of privacy invasion.

I think state officials are a ready and willing source of wisdom on this topic. And so, I think we need to be very, very careful in what we do here that may in any ways subplot what they're doing. Thank you Mr. Chairman.

WICKER: Thank you, Senator Blumenthal.

Senator Sinema?

SINEMA: Well thank you Mr. Chairman for holding this hearing.

Data privacy is an important topic for all Americans and I'm glad the committee continues to explore this complicated issue from all angles. Everyday, we learn about new misuses of Americans private data on the Internet including recent examples in the past month of millions of social media passwords being stored in unencrypted format.

So, this issue requires bipartisan solutions that protect the privacy and security of Arizonians while allowing innovation, creativity and investment to flow into new and emerging technologies and businesses. I'm particularly pleases hearing focuses on the impact of data privacy legislation on consumers. They are the ones who lives could have ended of passwords get hack, identities get stolen. And consumers should have the right to control their own private information.

A particularly vulnerable population to privacy abuses and identity theft are elderly Americans. The United States has COPPA, a specialized privacy law to protect children, but our seniors also experience elevated risks of having their data misuse.

Elderly American sometimes struggled to navigate the complexities of privacy policies and are often the targets of fraud. I want to make sure that any federal privacy law gives seniors in Arizona and across the country the tools they need to thrive in a digital economy. And the protections they need to enjoy a productive and secure retirement.

My first question is for Mr. Steyer, but I welcome the perspective of all of our witnesses.

So, thank you for your focus on children and the particular concerns they face. I think the consumer education piece is a critical aspect of any data privacy legislation. As you state in your testimony, many people who want to limit data collection by websites don't know how to do it, which is an issue of both transparency and digital literacy.

Can you give a brief overview of your digital citizenship curriculum and discuss whether you think any of these tools are appropriate or could be adapted to intricate older Americans?

STEYER: Yeah, that's a great question Senator Sinema. So, our digital literacy citizenship curriculum 75,000 members schools now, it's basically driver's ed for the Internet and cellphones. It sort of the basic rules of the road. And I -- it's -- I think your point about seniors is a great one because they didn't grow up with the technology.

It's hard for teenagers who are first generation native technology just to understand some of the stuff so why should a senior citizen? So, I think the importance of consumer education in simple clear ways to understand what your rights are. And then how to exercise them, it's basically digital literacy. And if you guys put this into the bill, we'll create a curriculum for you for all age -- age ranges in the country. It's a very good question.

POLONETSKY: And I'd love to see the FTC really taking a lead role. They have a business outreach department but as I see, if we do a lot working in Europe, the challenge frankly has been the huge number of small businesses that are sending questions, that are sending e-mails, that they don't need to send to ask for permission.

It's been a big transition. And if we're going to pass a new law and I hope we do, we should be ready to help the teacher who is creating an app because she thinks it's a better way to teach her kids so that she doesn't have to hire outside counsel. And I think the FTC certainly Common Sense and other groups, but I think the FTC in addition to giving in those enforcement stuffs, giving them those education outreach a critical.

SINEMA: Thank you.

GULIANI: I just to make a point, I think that the owners shouldn't be on the individual, right? I think you're question sort of speaks to a larger problem which is the complexities and difficulties that not just elderly Americans but everybody faces. And I think that that's one of the reasons we've supported an app in the framework instead of an opt-out, right?

When you talk about technical literacy, the difficulties someone may have and not only all of the apps they do business with, all of the entities who might have their data but how to navigate the complex framework of opting out. It's just too much of a stress to put on consumers, that why we've supported opt-in.

SINEMA: Thank you.

DIXON: I would agree that we shouldn't put too much emphasis in terms of the responsibility of the individual solely to protect themselves, but I think consumer education is very important.

The Data Protection Commission in Ireland has just closed the consultation in relation to children and the exercise of their rights and the GDPR. We consulted directly with the children through schools, we developed lessons plans which was impart in education of children around the uses of their personal data.

So, we very much believe in active communication to consumers through our websites, through the promotion of case studies, promoted by the media. And I think this is an important part of the jigsaw as well.

SINEMA: Thank you. Thank you Mr. Chairman.

WICKER: Thank you very much.

Senator Sullivan?

SULLIVAN: Thank you Mr. Chairman and I apologize to the witnesses for my late arrival but I wanted to make sure I was able to ask at least at least a few question on a very important topic. And what I want to do in and -- and again, if this is been covered, I apologize but wanted to focus a little bit more on the international aspects.

So, this is something that we had a hearing, actually a subcommittee hearing that I'd chaired yesterday with Senator Markey after our leader here set up a really important new subcommittee on economics and security. And the idea was kind of international standards and where we have typically lead in this area, the United States (inaudible) director was there and number of other witness at the subcommittee hearing.

But how do we -- how are we suppose to think through as we look at these privacy standards and the different standards internationally, obviously there's what's going on in Europe, but there's also concerns that I have even more broadly than just what's happening in Europe, is that when you have kind of the 5G race that's happening globally and Huawei in some ways leading that, that you might have a de facto leadership that relates to standards coming from China that to be honest in the world of privacy is a real concern I think even a bigger concern on the European regulatory framework.

So, how should we be thinking about this and trying to help make sure that what we're doing with our allies is the standard that we think is appropriate for, you know, countries like ours that are democratic capitalist countries?

STEYER: Senator Sullivan if I may, just two points.

SULLIVAN: Please and I open this up to all.

STEYER: A couple of points. One, when we wrote the California law last year, the CPPA which we've been talking about in the hearing, we met the folks who wrote GDPR and we realized that the values of the U.S. are in many ways similar to folks in the EU but they're different in certain areas.

So, we were very careful and I think that this can be done here at the federal level as well to think about how there are certain areas like the first amendment we're talking about this earlier that may mean that a privacy law in the United States will be slightly different than GDPR. But most of the protections are universal.

That said, you can modify...

SULLIVAN: Universal relative to liberal democracy?

STEYER: Exactly. That was I was going to say. And the second thing is not -- I'd be willing to bit you a large sum money that Huawei will not dominate the 5G universe and I mean that.

SULLIVAN: Why?

STEYER: Because I think...

SULLIVAN: I'm glad you're so optimistic.

STEYER: Because the technology in the United States and the companies in the United States have brought this world the extra ordinary advances. That doesn't mean we don't need to be aware of this but sacrificing important privacy reductions for consumers just because China might do that would not be smart strategy.

And I think at the end of the day, a strong deferral privacy production which where the California laws is the floor and where you really take into consideration the fact that most of the companies that matter are here in the United States will give us the protections that we need.

SULLIVAN: Other thoughts on that?

(CROSSTALK)

POLONETSKY: Please go ahead.

GULIANI: I was going to say, I mean I think that we can take some lessons from GDPR. Regulation in the U.S. is not going to look exactly the same as Europe. There is concern or the right to be forgotten and changes that would need to be made to be consistent with the U.S. constitution, the enforcement framework will look different.

And also in the U.S., we have state level actors. Attorney generals, agencies, legislators, and I'd think the last thing we want to do is we weaken the ability of those actors who have a long history of working on this issues of sort of having a sit at a table and being able to enforce and create good laws.

But having said that, there are positive elements of GDPR that we should take and learn from, the extent to which places rights in the hands of consumers and increases standards around consent and limits on how...

SULLIVAN: Let me just -- real quick and then I'd like to hear the all sharing (ph) but none of you are advocating for state-by-state approach to this, are you?

STEYER: No, but we were very clear that we have deep skepticism about preemption, if there was going to be a water down federal law that would say, lessen the protections you have at the baseline of California. That was the discussion we had.

POLONETSKY: We're just to look to the Asia Pacific allies that do have. So, we've had a leadership rule in the APEC process where we've work with Japan, Korea, a number of the major economies similarly want to cooperate with data protection flows, the US recently, you will be considering the new NAFTA treaty. We committed to use the APEC CBPRs, the APEC process to move data across North America.

So, GDPR obviously important place center but we've been leaders in the OECD which has an important set of privacy frameworks and we been very active throughout many administrations in the APEC process and those are two regimes we should look to for global cooperation.

SULLIVAN: Great. Thank you Mr. Chairman.

WICKER: Thank you Senator Sullivan.

There's a vote on.

Senator Cruz is recognized and preside (ph) for a time.

Senator Cruz?

CRUZ: Thank you Mr. Chairman.

Thank you to each of the witnesses for being here.

There's no doubt that protecting privacy is critically important and how we should do so. What government regulation should be in place concerning privacy? It's going to be a policy question that suspect will be with that a very, very long time.

At the same time that we want to protect privacy, we also want to avoid a regulatory system that imposes unnecessary burdens and that threatens jobs. And I think there are lessons that we can draw based on the experience we've seen elsewhere. There's been considerable discussion here about the European Unions general data protection regulation GDPR.

In November 2018, the National Bureau of Economic Research found that, "The negative effects of GDPR on technology investment appear particularly pervasive for Nissan 0 to 3 years old ventures which may have cost European start ups as many as $38,000 techs jobs."

Even more alarming the report goes on to state, "The potential for job losses may well extend and intensify past our four months post GDPR data set period." In which case, the effects on job is understate. And the weak of GDPR California enacted its own law, the California Consumer Privacy Act for 2018. And according to the international association of privacy professionals the California Privacy Act will affect more than 5000 US companies. The vast majority of which are small to medium size enterprises.

What lessons should this committee or should Congress take from the experience with GDPR and the experience with California Privacy Act?

STEYER: So, Senator Cruz, I'm Jim Steyer and I -- we basically wrote the California Privacy Law with the legislature there. I would tell you the bottom line lesson is that privacy is good for business.

We wrote that law really with some of the most important tech companies in the United States, Apple, Microsoft, Salesforce but I ran a small business, right with several hundred employees, we have to comply with the California law and GDPR. And we think and so -- I run a small business and no -- the fact that it does matter.

But in the long run, I think what you saw because you had unanimous by partisan support in California among all the Republican legislatures as well as Democratic legislatures to support it.

So, I would say, well-crafted strong privacy protections are in the best interest of business and I think that the record speaks for itself in that regard and you should feel confident that a smart Congress just like a smart California legislature will find the right balance on that.

CRUZ: So, let me focus of a second on the GDPR piece, the witnesses agree that the GDPR regulation is having or had a significant negative effect on jobs and are there lessons that we should derive from that?

POLONETSKY: I think Senator one easy lesson that we can take and improve on as we look at how to legislate in the GDPR, the European Data Protection board is issuing quickly but frankly it's a year end is issuing opinions on some of the core provisions of the GDPR.

There is an opinion out now that's not yet final on what can be in a contract. And obviously that's a core thing, lots of companies are doing their business based on contract and we won't have final guidance and it's a year out.

So, the more we can do to give clarity here or the rules and yeah there's room for rule making in the areas that are complex and they haven't been figure out but I should be able to comply the day, the law passes. There's some -- there's a real overhang of uncertainty in a number of areas where the board has yet to issue opinion, so people actually know what the rules are.

GULIANI: Yeah. And I don't think that their -- it's necessarily that a privacy law is going to hurt small business. I do think that a law should reflect the realities of small business. So, for example penalties, you might want to have different penalties based on the size of the business or the amount of data they hold.

And I do think that there are some rumors and myths around the extent to which GDPR harm some businesses. I'll give you a good example that's been reported. You know following GDPR, New York Times reportedly stop doing targeted advertising in Europe and did contextual advertising. They didn't find that their advertising dollars went down, they went up.

And so I do think that there are ways that businesses can respect privacy and make a profit and we're starting to see businesses that are innovating around that, right? DuckDuckGo, who's trying to create an alternative to Google that respects privacy. So, this also an industry to I think promote privacy and create right respecting products.

STEYER: And Senator Cruz, I would tell that we've been spending a fair amount of time talking about the incredible importance to your family, my family and everybody in this room's family and ourselves about the protection.

And I -- having -- living in the state where most of the big and small tech companies are based and working with them, I think they have now come to the conclusion that while there maybe some modifications that need to be made, which is the normal legislative rule making process, in the long run, this is good for business and it's good for consumers and it's good for everybody.

So, I think I agree with Ms. Guliani that I think some of the statements about job loss et cetera have been overstated. And that the value of a quality privacy regime for the Cruz family, the Steyer family and everybody else is totally worth it.

DIXON: Senator, equally at the Irish Data Protection Commission were not aware of evidence that the GDPR is affecting jobs adversely.

I spoke earlier about risk-based approach that the GDPR endorses and it does give a knowledge to smaller and micro enterprises. And it provides for implementation only of the organizational and technical measures that are appropriate and proportionate to the risks of the personal data processing operations in question and to the scale of the organization.

So, I think approached and implemented at it's intended it should do the opposite of effect jobs, it should engender better consumer trust and a more sustainable business model.

CRUZ: Well, I want to thank each of the witnesses for your testimony. This testimony has been helpful.

The hearing record, it will remain open for two weeks. During that time senators are ask to submit any questions for the record. And upon receipt the witnesses are requested to submit their written answers to the committee as soon as possible, but no later than Wednesday, May 15th, 2019.

With that, I thank each of the witnesses for testifying and the hearing is adjourned.

END

May 03, 2019 18:09 ET .EOF