Mar 14 2019 11:08:07
TRANSCRIPT

March 12, 2019

COMMITTEE HEARING

SEN. LINDSEY GRAHAM, R-S.C.

WASHINGTON, DC

SENATE JUDICIARY COMMITTEE HEARING ON GDPR & CALIFORNIA CONSUMER PRIVACY ACT: OPT-INS, CONSUMER CONTROL, AND THE IMPACT ON COMPETITION AND INNOVATION

Bloomberg Government

Support: 1-877-498-3587

www.bgov.com

SENATE JUDICIARY COMMITTEE HEARING ON GDPR & CALIFORNIA CONSUMER PRIVACY ACT: OPT-INS, CONSUMER CONTROL, AND THE IMPACT ON COMPETITION AND INNOVATION

MARCH 12, 2019

SPEAKERS:

SEN. LINDSEY GRAHAM, R-S.C., CHAIRMAN

SEN. CHARLES E. GRASSLEY, R-IOWA

SEN. JOHN CORNYN, R-TEXAS

SEN. MIKE LEE, R-UTAH

SEN. TED CRUZ, R-TEXAS

SEN. THOM TILLIS, R-N.C.

SEN. BEN SASSE, R-NEB.

SEN. MICHAEL D. CRAPO, R-IDAHO

SEN. JOHN KENNEDY, R-LA.

SEN. JOSH HAWLEY, R-MO.

SEN. JONI ERNST, R-IOWA

SEN. MARSHA BLACKBURN, R-TENN.

SEN. DIANNE FEINSTEIN, D-CALIF., RANKING MEMBER

SEN. PATRICK J. LEAHY, D-VT.

SEN. RICHARD J. DURBIN, D-ILL.

SEN. SHELDON WHITEHOUSE, D-R.I.

SEN. AMY KLOBUCHAR, D-MINN.

SEN. CHRIS COONS, D-DEL.

SEN. RICHARD BLUMENTHAL, D-CONN.

SEN. MAZIE K. HIRONO, D-HAWAII

SEN. CORY BOOKER, D-N.J.

SEN. KAMALA HARRIS, D-CALIF.

WITNESSES:

WILL DEVRIES, SENIOR PRIVACY COUNSEL FOR GOOGLE, INC., MOUNTAIN

VIEW, CALIF.

ALASTAIR MACTAGGART, CHAIRMAN OF CALIFORNIANS FOR CONSUMER

PRIVACY, SACRAMENTO, CALIF.

DAVID HOFFMAN, DIRECTOR OF SECURITY POLICY AND GLOBAL PRIVACY

OFFICER FOR INTEL, SANTA CLARA, CALIF.

GABRIEL WEINBERG, CEO AND FOUNDER OF DUCKDUCKGO, PAOLI, PA.

TOM LEE, POLICY LEAD FOR MAPBOX, WASHINGTON, D.C.

ROSLYN LAYTON, VISITING SCHOLAR AT THE AMERICAN ENTERPRISE

INSTITUTE, WASHINGTON, D.C.

MICHELLE RICHARDSON, DIRECTOR OF THE PRIVACY AND DATA PROJECT

AT THE CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, D.C.

AND JANE BAMBAUER, PROFESSOR OF LAW IN THE UNIVERSITY OF

ARIZONA JAMES E. ROGERS COLLEGE OF LAW, TUCSON, ARIZ., TESTIFY

GRAHAM: The hearing will come to order.

So, about a year ago we had a joint committee hearing with the Commerce Committee with Facebook CEO Mark Zuckerberg to try to find out what role Congress should play, if any, dealing with privacy issues around social media companies and outlets.

And as you fast forward, Europe has acted and we're here to learn what Europe did and see if it's working, helping or hurting. I think the acronym is CDPR (sic). California is about to pass a law that goes into effect in January, we're trying to learn from our friends in California about their approach to this problem.

To the Commerce Committee, I realize this is your primary jurisdiction, but I'd like to work with the Commerce Committee, we had a joint hearing for a reason because there are some crossover jurisdictions. But the content part seems to be mostly us. How you protect the platforms seems to be mostly us. Most of the privacy issues I think are in Commerce, some in Judiciary.

But the big picture for me is I want to make sure consumers understand what's happening when they sign up, that they're basically monetizing you. That's how they make money. If they don't charge a fee, all your interactions on social media is used by the media companies to sell advertising.

And we just want to make sure that people understand what they're signing up for and how far this goes, and what's too far. And I don't have any of the answers by any means, but I certainly believe the problem is real.

On the content side, many of you are having to make decisions about what to put up, what to take down. What's hate speech, what's not? What's too provocative with absolutely no guidance from your government?

And you're neutral platforms, nobody's holding you responsible for what you put up. Nobody's holding you responsible for what you fail to take down. But that's a big advantage in the law. If you have a newspaper, a TV show, a TV station, you can be regulated and you can be sued.

I don't want to destroy the goose that laid the golden egg in terms of innovation. I think all these social media outlets have enriched our lives, but there's a downside and potentially a dark side when they can be manipulated by foreign powers, terrorist organizations in a fashion to cause harm here at home.

We have a very talented committee of Republicans and Democrats, and this is one area I think there's a lot of bipartisan desire to learn more and to do something constructive.

So with that, I will turn it over to Senator Feinstein for any statement she would like to make.

FEINSTEIN: Thank you so much, Mr. Chairman.

I want to be clear, I think protecting individual privacy is critical, and we must do all we can to give people control over their data. The two laws that we're reviewing today are the European Union's General Data Protection Regulation and California's Consumer Privacy Act. Our goal in this hearing should be to understand what impact these laws are having and how well they're protecting our consumers.

It's useful to remember, I think, what has brought us to this point. In the past few years, hundreds of millions of consumers have had their sensitive, personal data stolen as a result of data breaches. The Equifax breach in 2018 compromised data for 146 million individuals. The Yahoo breach in 2014 and the Marriott Starwood breach in 2018 each affected half a billion people worldwide.

Consumers are now just becoming aware how insecure our personal information is with the expansion of smart phones, online services, and even appliances in our homes and offices that we regularly use.

For example, programs on smartphones can use geographic information to figure out where we are at any given moment and then sell it to nearby retailers and restaurants vying for businesses that want to promote coupons and discounts to entice individuals to buy from them. This can be a good thing if it's done with the approval of the consumer.

Last year, the New York Times revealed that there is now a thermometer to collect fever and symptom information from families and then sell that user data, and it was sold to Clorox. Clorox identified which zip codes were showing increases in fevers and directed more ads for products like disinfecting wipes to those areas.

While this kind of targeting may have had a benefit for consumers, it also has very serious implications for personal privacy, especially when the data involves medical information. The reason this was in the news at all is that it crosses a murky line on how we reasonably expect online services to use very sensitive information that we entrust to them.

I represent the State of California, birthplace to some of the most innovative companies in the world at the heart of the internet revolution. California though is also home to some of the most heavily criticized companies for their collection of personal data, and as a result California is home to the strongest state privacy law in the nation. In fact, one of our panelists -- where are you, Alastair MacTaggart -- seated before us today assisted with the drafting of this law.

Europe's law went into effect last year impacting virtually every company of any size operating in Europe. Companies are also gearing up to comply with California's law which will go into effect next year, and that must happen. There has been some push back against these laws with companies saying the requirements are too cumbersome to comply with, and the penalties too stiff for even unintentional violations.

In addition, some complain that the opt-in consent requirements in the European law result in confusion to consumers. Others have complained that California's law is too narrow, and does not go far enough to limit abuses by companies that collect data from the consumer directly.

Let me say again, it's my belief that individuals should have as much control as possible over their personal data. I commend the California law for protecting most California residents. But I also believe affirmative opt-in consent should be the standard, and that's a position I have taken for years. Not opt-out.

Companies should also be required to protect their company's -- their customer's personal data with a heightened degree of care, and should be held responsible should that data directly or through cyber breach end up in the wrong hands.

I will not support any federal privacy bill that weakened the California standard. I also believe that any federal legislation should include data breach notification requirements. I have had legislation on this issue, Mr. Chairman, going back to 2003.

GRAHAM: Wow.

FEINSTEIN: And get it through, and that's notifying people...

GRAHAM: Terrible.

FEINSTEIN: ... when their data is breached.

You're right, it is terrible.

Consumer data privacy is a fundamental issues facing all of us. I welcome the discussion from our panelists to hear about their views on the pros and cons of these laws.

And Mr. Chairman, I want thank you for this hearing and have the Judiciary Committee begin to hear more about this important topic. You know, as all of the high-tech spreads, the protection for people's rights increases, and medical data protection I think heads the list. So thank you very much.

GRAHAM: Thank you, Senator Feinstein.

Would you please rise and raise your right hand? Do you solemnly swear that the testimony you're about to give this committee is the truth, the whole truth and nothing but the truth so help you God. All right.

We have Mr. Will DeVries, is that right? How do you say it?

DEVRIES: DeVries, Senator.

GRAHAM: DeVries, OK. He's the senior privacy counsel for

Google. Alastair MacTaggart, chairman of Californians for Consumer Privacy. David Hoffman, director of security policy and global privacy officer, Intel. Gabriel Weinberg, is that right? CEO and founder of DuckDuck Company. Tom Lee, policy lead, Mapbox, Inc., Washington, D.C. You've all lived distinguished lives and I could have (ph) gone on longer, but that's enough. All right.

DEVRIES: Chairman Graham, Ranking Member Feinstein, members of

the committee, thank you for inviting me to your -- to appear before you this morning. My name is Will DeVries. I'm a senior privacy counsel at Google. I've worked at the intersection of privacy, technology and the law for 15 years including teaching privacy law at the George Washington University of Law School. At Google I advise on global data protection compliance and product development.

Google's approach to privacy and data protection stems directly from our founding mission, to organize the world's information and make it universally accessible and useful. A key part of fulfilling that mission is building products for everyone regardless of their economic circumstances. And to this end, many of our products are free with -- with advertising as our main source of revenue.

These products and services provide tremendous value to users and businesses across the globe, but if our users don't trust us, they won't use our products. Protecting the privacy and security of our users isn't just a compliance strategy or a slogan. It is vital to our business.

Google aims to continually improve our approach to privacy and enhance the transparency and control and security that we build into our products. We have many years of practical experience building systems that apply our privacy principles in the U.S. and around the world, and there is more momentum for and consensus around creating a federal privacy law than at any time I've seen in my career in privacy.

Google welcomes this and reaffirms our longstanding support for a smart, strong, comprehensive privacy legislation.

Legislation would codify important individual rights and help promote and sustain U.S. global leadership around the free and open internet including promoting cross-border data flow and compatible pro-privacy and pro-innovation rules in other countries.

We believe there are a number of key components that Congress should consider as it drafts comprehensive privacy legislation. At its core, legislation should be risk and outcomes based, consistent, adaptable, and work for all types and sizes of entities. It should apply to all businesses and organizations that process personal information, and all data that can be used to identify an individual.

I want to briefly cover five key aspects of comprehensive privacy legislation. These aren't the only things that would go in a comprehensive bill, but in the interest of time I'll focus on these.

The law should require responsibility and reasonable data collection in use. We think that businesses and organizations should protect against potential risks and balance the legitimate interests of their -- of the organization processing the data against the impact of the processing on the rights and interests of the individual.

The law should require transparency. As a baseline companies and organizations should provide notice about the types of personal information they collect, why they collect it, how they use it and disclose it, and particularly when it's used to make decisions about an individual. And there should be incentives to go beyond the privacy policy and actively inform users about data use in the context of the services themselves.

The law should require choice and control. People have different preferences about how they want their information to be used, and preferences can vary over time. Federal privacy law should require

businesses and organizations to provide appropriate mechanisms for individual control including the opportunity to object to data processing where feasible in the context of the service.

The law should require portability. In addition to rights like access, correction and deletion, privacy laws should also ensure that individuals where practical can download and export their personal information. This not only empowers individuals, it also keeps the market innovative, competitive and open to new entrants.

Lastly, the law should require accountability. A privacy regulatory framework should have strong enforcement and prioritize outcomes over process. The law should encourage diverse and innovative approaches to compliance and to privacy protections.

To give detail to our call for comprehensive privacy law, we recently published a framework for data protection regulation, and provided additional detail and comments with -- to the Department of Commerce, both of which I've included in my written submissions.

We also encourage a review of the numerous established privacy principles and frameworks which have much to offer such as the Fair Information Practice principles, the OECD privacy principles, the APEC privacy framework and the European GDPR to understand what's working, what can be improved and how to support international interoperability for U.S. companies that operate abroad.

In conclusion we believe the continued success of services that collect or use personal information depends on individual's trust, that their information will be protected. We look forward to constructively engaging with Congress and other stakeholders as you consider privacy legislation that will continue to build and maintain that trust.

Thank you again for the opportunity to share our perspective and experience, and I welcome your questions.

MACTAGGART: Chairman Graham, Ranking Member Feinstein, and

distinguished members of the committee, thank you for inviting me to come testify before you today. It is an honor and a privilege.

I come to you as the person who created and sponsored a ballot measure in California last year which resulted in the passage of the California Consumer Privacy Act, or CCPA. I also come to you as the father of three little children concerned about the world they're growing up in where potentially every step and test they take will be tracked and sold to hundreds of companies they've never heard of.

And finally, I come to you as a business person. I believe that our freedom depends on our prosperity, and I would never have undertaken this journey if I didn't believe it would increase business competition which I think is good for consumers and commerce.

So CCPA has three main components, three legs of the stool as it were, and they are, one, we get to find out what information corporations have collected about us. Two, we can tell those companies to stop selling our information. And three, companies have to keep our data safe.

Now CCPA builds on some of the best work done by some of the best minds at the intersection of computer science and privacy. For example, we borrowed heavily from something called Do Not Track which is an almost decade-long effort that began in 2009, and Do -- Do not Track was meant to give consumers a way to stop their browsing history -- their browsing being tracked. And while it worked technically, ultimately, it failed because it was voluntary.

So CCPA creates a similar provision to Do Not Track and gives consumers the ability to require businesses not to sell their personal information, and it does so in user friendly fashion, that doesn't take much work from consumers. So I think this spells the end of large data-mining companies tracking you pervasively across the web.

So this means that CCPA will help increase competition. How? Well, currently over 90 percent of new growth in digital ad revenue is being captured by two companies.

Smaller businesses that create content are being devastated. Why? Well, the huge platforms learn about us by tracking us on basically every site we ever visit, whether we're logged into them or not, whether we even have an account with them or not. And then they wait to show us ads on their own sites diverting ad revenues to where they make the most money.

So let me repeat that. They let independent sites do much of the work of creating content, and then while tracking us, they learn what we're interested in and then they use that knowledge to advertise to us on their own sites.

Now, that makes a ton of sense from their point of view, but you only have to look at the state of the nation's news businesses to see where this trend is going and to know that the ability to stop this third-party tracking, this pervasive tracking is going to benefit competition.

Now speaking of advertising, it's important to state that CCPA permits advertising. We didn't want to stop the engine that powers the internet. But we put limits on ads. So no longer will every ad you see, whether you click on it or not mean your personal information has just been sold or disclosed to thousands of companies you've never heard of.

Now how about GDPR? Well, unlike GDPR, CCPA only covers big businesses and data brokers. Unlike GDPR's opt-in approach, CCPA is opt-out which we feel both makes for a better user experience and we think it improves privacy. There's no click fatigue from the incessant popups, and more importantly, there's no take-it-or-leave-it approach requiring consumers to consent in order to use the service.

In summary, CCPA is balanced legislation and gives consumers a meaningful control over what happens to their personal information. That's why the data miners are asking this committee for preemption because they're concerned about a threat to their business dominance.

In closing, let me remind you that every day huge corporations are tracking us across our digital footprint. Their algorithms classing us -- classing us as whether we're considering divorce, about to get pregnant, or a persuadable and gullible voter. Every mouse click and search goes into a digital file that dwarfs what any intelligence agency has ever known about its citizens in history.

Now I understand this committee is considering national legislation, but I urge you not to undo CCPA's protections which now cover one in every eight Americans. Almost 630,000 registered voters signed the petition which never polled below 80 percent. And the law passed out of both houses of the California legislature unanimously.

That's right, not a single Republican or Democrat voted against it and why is that? It's because privacy is not partisan.

So thank you for your time, I feel sure that as dedicated public servants you share my desire to give Americans the ability to take meaningful control over their and their children's personal private information.

HOFFMAN: Good morning Chairman Graham, Ranking Member Feinstein

and members of the committee, thank you for the opportunity to testify today. I'm pleased to address the committee on the need to put in place a national privacy law that protects people more and better than GDPR and CCPA.

Intel's bringing artificial intelligent technology to market to provide individual and societal benefits. The U.S. needs a law allowing for access to data to enable innovative companies large and small to develop artificial intelligence products and services.

GDPR and CCPA have substantial negative impacts to innovation and competition, and a new model is needed. In short, we need a uniquely American law that is stronger and better than GDPR and CCPA.

A recent television news report interviewed a woman named Donna, a survivor of domestic violence whose identity they protected for her safety. Donna had recently discovered her name and address on a data broker's site. Donna told the news team if you have someone who's tried to kill you, for them to be able to just type in your name and any known address that you've stayed at can pop it, it's scary because now they know ways to start trying to find you.

Victims of domestic violence are not the only ones at risk. Data broker lists include police officer home addresses, contact information for rape survivors, information on seniors who suffer from dementia, and specific categories allowing for racial and ethnic discrimination.

None of these people chose to place their names and contact information on these lists. They likely don't even know that those lists exist. The current environment makes clear that the notice and choose method of privacy protection only provides choices for those that want to profit off the pain of Americans. Data brokers are selling the safety of the American people online for $9.99 and lower.

The American people insist that this must change. Following the European Union's General Data Protection Regulation, Californians started the ballot initiative that turned into the California Consumer Privacy Act of 2018. Now there are 94 other state privacy laws at some point in the process of discussion and introduction.

Unfortunately, GDPR and these state laws are both unlikely to adequately protection Donna while they also risk the promise for social improvement and economic progress from new technologies like artificial intelligence.

These laws wrongly assume that individuals can exercise consent over how their data will be used. The data broker lists I mentioned largely draw from public records or information scraped from websites and social media applications. Laws focusing on collection of data directly from individuals are already outdated and will become even more so as improved analytics are used on data available from data brokers or on the internet.

These notice and choice laws create barriers to innovation and competition. The patchwork of state legislation will create significant new barriers to the innovative use of data. Only large law firms benefit from this patchwork because businesses of all sizes will need lawyers to determine how to offer products and services nationwide. These legal costs will slow small, innovative data-oriented startups.

A new model of privacy protection that does not rely primarily on consent is needed. For 50 years Intel's relied upon two things for our success. First, innovative companies that develop new products and services using our technology. And second, individuals having trust and confidence in their use of their products and services.

The current data broker environment and the resulting legislative patchwork puts both of those elements at risk. Data brokers are poisoning the well of trust out of which real technology companies like Intel and our customers must drink. For that reason, Intel created a model for privacy legislation and we ask that Congress use it to do three things.

First, provide meaningful protections instead of the false promise of control. Second, prohibit unaccountable data sharing with third-party companies. And finally, empower and fully resource the Federal Trade Commission.

In conclusion, a law based on Intel's model will provide the protections people erroneously believe are provided by GDPR and CCPA without the negative impacts to competition and innovation. Intel's proposal provides strong protections and robust enforcement while still allowing for the innovative use of data to allow artificial intelligence and other technologies to fulfill their promise.

I encourage you to use our framework to put in place a law that will optimize for the ethical and innovative use of data and will protect Donna. We stand ready to support the committee's effort to advance legislation. Thank you.

WEINBERG: Chairman Graham, Ranking Member Feinstein, and

members of the committee, thank you for inviting me here today. I'm here to explain that privacy legislation like GDPR and CCPA is not only pro-consumer but can be pro-business and even pro-advertising.

DuckDuckGo's primary service is a search engine alternative to Google that allows you to search the web without being tracked. We're the fourth largest in the U.S. and we do about a billion searches a month. We also offer an alternative to Google Chrome which is a mobile privacy browser.

Now I founded DuckDuckGo in 2008 pretty far outside Silicon Valley in Valley Forge, Pennsylvania. And we now have, I'm proud to say, a distributed workforce across ten states and ten other countries and D.C.

We're here today because the American people are pretty much tired of being tracked online everywhere they go. They're tired of the invasive ads, data breaches, discrimination and manipulation. I'm sure everyone here has had the same shared experience of searching for something and then have that thing haunt you around the internet, especially on apps that you visit.

Well, DuckDuckGo is here to help -- help you avoid those types of scenarios. In particular, every time you search on DuckDuckGo, it's like the first time you've ever been there. We don't even have a concept of a search history. We also offer privacy protection beyond the search box, so when you go and visit web pages, there's all these hidden trackers kind of lurking behind the scenes based on these invasive tracking networks. We block those hidden trackers.

Now in many ways I come to you from the future. I run a business that's already CCPA and GDPR compliant. Our privacy policy is extremely straight forward, and doesn't require any kind of law degree to decipher.

In fact, it's this simple. We do not collect personal information at all. Yet, even with this simple privacy policy, we nonetheless are able to make money through advertising which brings me to my first point, that privacy legislation is not anti-advertising. In fact, I'm proud to say we've been profitable since 2014, and although our finances are private, we are subject to the CCPA's floor or revenue restriction of $25 million.

So take DuckDuckGo as an example for adverting. When you search on DuckDuckGo, we can show you ads just based on what you searched on. So if you searched for a car, we can show you a car ad knowing nothing about you as a person. This is contextual advertising based on the search and not based on you as an individual.

And we're not alone. For example, the New York Times following GDPR changed their site in Europe to stop behavioral advertising and move back to contextual advertising based on what is in the article, and they reported an increase in revenue, not a decrease. And just last week, Business Insider reported that Washington Post was looking into something similar.

My second point is that privacy is actually good for business. Consumers are flocking to brands that they trust and respect. According to Harris Poll, data privacy is actually the most pressing issue on Americans' minds now for the second year in a row believe it or not. And we stand testament to that as a case in point because we've been growing exponentially during this time period.

My third point is that well-drafted legislation can actually spur competition and innovation in what is arguably the central market in the internet which is the digital ad market. Right now this ad market is a duopoly and it's hurting all kinds of businesses. It's hurting small businesses, venture-backed companies as well as the largest media companies.

To restore competition in this market, these data monopolies at the core need to be addressed. Now fixing that could take a bunch of forms, but here are three suggestions.

First, consumers should be given a real robust mechanism to opt-out of data tracking, especially by these companies at the center of these monopolies. Second, monopoly platforms should be prohibited from combining data across their different business units. And third, acquisitions that strengthen the data monopolies should be prohibited.

Our mission at DuckDuckGo is to raise the standard of trust online, that's exactly why we support strong privacy legislation. We believe the internet shouldn't feel so creepy, and getting the privacy you deserve online should be as simple as closing the blinds. I'm happy to answer any questions, and thank you again for inviting me to the hearing.

LEE: Chairman Graham, Ranking Member Feinstein, members of the

committee, thank you for the opportunity to appear before you today. My name's Tom Lee. I'm an engineer by training and I now lead policy at Mapbox. Today I'd like to talk to you about how our company approaches privacy, and how privacy reforms should approach smaller companies like ours.

We make maps, and our customers are developers. We power weather forecasts, messaging tools and major news sites. You've probably used our maps. In total we serve over 520 million monthly active users.

Our users benefit from our maps and we benefit from their use. By collecting GPS data we make those maps more accurate, we detect traffic jams, and we give better directions. We built these features, though, knowing that we had a responsibility to put user privacy first.

We work to minimize the information we collect, we anonymize what we do collect. We require our customers to let their users opt-out of collection. We encrypt the data in transit and at rest. We apply strong access and control policies, and we only use the data to make our products better. We're in the business of selling maps, not information about the individuals who use them.

Our success proves that you can build a valuable business and protect user privacy at the same time, and we're glad to see growing attention to this issue from lawmakers in this body, in state legislatures and around the world. We think it's time for some rules of the road, common sense ethical standards for anyone that asks users to trust them with their personal data.

But new regulations inevitably carry costs and risk, especially for smaller businesses like ours which aren't among the names we're all used to seeing in headlines about privacy. I'd like to highlight some issues that deserve attention as you consider how to craft reform without harming competitiveness or innovation.

First, the burden imposed by a proliferation of varying privacy standards is real. Our small but mighty legal team has to handle customer contracts, patents, employee policies, vendor agreements, scores of other issues.

Proceeding through the GDPR compliance process cost us hundreds of hours of efforts initially, and continues to introduce (ph)

initial time and complexity as we negotiate deals with customers. Startups can't afford to multiply that cost by dozens of additional jurisdictions, especially if some of those future regulatory regimes prove to be in conflict with one another.

We believe that our nation's privacy laws should be strong, and that they should be unified. We favor a single, national standard. Avoiding a patchwork of state rules will not only help smaller businesses like ours, but will give Americans assurances that don't change when they cross the state border.

Second, a jumble of state privacy laws risks creating loopholes, oversights and errors. It's easy to see why when you consider how much of our conversation on privacy is focused solely on the tech giants whose apps are used directly by billions of end users.

The California Consumer Privacy Act is a good example of a law that is very well designed, thanks to the experts brought to bear on the initial ballot measure. But still fails to completely imagine businesses like Mapbox.

For example, some of our customers run vehicle delivery fleets and they use our technology to monitor how -- monitor how efficiently those deliveries are being made. Under the CCPA, the drivers in those fleets could request data about their employers' operations, even if they've since left to work for a competitor.

Exposing trade secrets isn't what the CCPA was designed to do, and we're hopeful this problem can be fixed in rulemaking. But we worry that similar oversights will be inevitable if state laws proliferate in the absence of a clear, federal standard.

Third, poorly designed reform could entrench big business and harm smaller companies. Unlike some of our competitors, we don't own a major mobile operating system. We collect anonymized data when people use maps in our customers' applications.

The platform owners can collect data at a much lower level than this, and reform that fails to adequately protect secure and ethical data collection like ours risks creating uncertainty among our customers and a chilling effect. If that were to happen the accuracy of our maps and driving directions would suffer which would make it much harder for us to compete with those platform owners.

Finally, some well-meaning reforms could actually put users at greater risk by forcing collection of more user data. Data export and deletion requirements in particular often fail to envision businesses

like ours. We rarely have a direct relationship with end users. We don't know their names, e-mails, phone numbers or other personal details. All we collect is anonymized data and metadata like IP addresses which are inevitably part of any internet request.

But privacy reforms efforts including the CCPA and GDPR name those IP addresses as personal information, and include data export and deletion provisions that are associated with personal information.

This combination opens the possibility for requests filed by identity thieves, vandals and abusers. To reliability detect illegitimate requests, we might need to collect much more personal information about users than we do today, putting us and them at greater risk. It would be ironic if privacy reform led to more collection of personal data rather than less.

I know some of these concerns are technical and specific. I mention these details only to make a larger point. We agree that Americans deserve stronger privacy guarantees, but the details are critically important, and it'll be easy to get them wrong.

This work needs to be pursued in a unified and careful manner in a way that minimizes the opportunities for mistakes. Businesses subject to new rules will deserve detailed guidance about how to comply, and the people depending on these rules will deserve a system with the flexibility to respond to new problems in the future. We think the work of privacy reform can bring a real benefits to Americans and we're eager to do whatever we can to support it.

I thank you for the opportunity to appear before you today, and look forward to any questions you might have.

GRAHAM: Thank you, all, very much. That was very, very helpful

actually.

Mr. Weinberg, if I were using your service and ask a question who won the most major golf tournaments on the PGA and you gave me an answer, how would you make money?

WEINBERG: So, Senator, we might show an ad that was related to

golf because...

GRAHAM: Because that's what I asked about?

WEINBERG: Yeah, exactly.

GRAHAM: How much would that effect Google if you were limited

to doing it that way? How much money would you lose?

DEVRIES: Senator, most of the revenue we make on advertising

comes from search ads as you talked about, and most of that is based just on the current search query. It's -- it's not too dissimilar from what Mr. Weinberg describes.

GRAHAM: So do you agree with that, California guy?

MACTAGGART: I think contextual advertising is the business that

built Google and Facebook. I -- I -- I think it's -- I agree with Mr. Weinberg, and it -- and it's -- there's nothing objectionable at all. People expect it.

GRAHAM: OK. So if I'm asking about cars, you'll show me a car

ad. If I'm asking about golf, maybe this person wants to know something about golf. This taking everything who am I, what kind of movies I like, you know, my politics, whatever, who does that, and how do they make money off of it, Mr. MacTaggart?

MACTAGGART: Well, so it's called behavioral advertising, and

they're trying to figure out everything about you so they can anticipate...

GRAHAM: Who are the companies that do that?

MACTAGGART: Oh, Google, Facebook, all the -- all the large

platforms.

GRAHAM: Well, he -- he said he didn't do that.

MACTAGGART: I-- I think he saying the -- what he said was the

majority of the money that they make now is...

GRAHAM: What percentage of your money is behavioral

advertising?

DEVRIES: I -- Senator, I don't have that number off hand, but I

can tell you that the -- the -- the value of behavioral advertising for those users who -- who have that setting on and who ask for that, that's a smaller percentage of our advertising revenue. I -- I don't know exactly the number.

GRAHAM: But you don't know how much it would be if it were just

-- took that off the table?

DEVRIES: No, I -- what I can tell you is that for -- for

operations like Google, most of our -- of our advertising is -- is based on the contextual information, the page you're visiting.

GRAHAM: Can you get back to me and let me know how much of it

comes from behavioral?

DEVRIES: I can follow up with you, yes. Absolutely.

GRAHAM: OK.

Mr. MacTaggart, so tell me what -- finish your thought.

MACTAGGART: Well, so CCPA explicitly would permit contextual

advertising because I -- again, people are -- are -- are not not expecting it, and I -- and we didn't want kill the engine that powers the internet. So there's nothing objectionable about that. What people find creepy is when it starts to anticipate, you know, who you are. So you're the single mother...

GRAHAM: Does it prohibit behavioral advertising?

MACTAGGART: No. What we do is we allow you to stop being --

your information being sold by these companies, and that's a way to stop these big, massive files being...

GRAHAM: When it comes to behavioral advertising, the consumer

gets a voice?

MACTAGGART: Absolutely.

GRAHAM: Mr. Hoffman, does -- does the Intel plan, how does it

work based on my question?

HOFFMAN: The -- the Intel model doesn't prohibit behavioral

advertising unless the use of behavioral advertising would create a substantial risk to the individual beyond what the individual's reasonable expectations. What -- what the Intel...

GRAHAM: Well, what is my reasonable expectation?

HOFFMAN: Well, I think your reasonable expectation is that

you're going to get the kind of advertising that's going to tell you about products and services that you're interested in, but you're not going to get advertising that's going to discriminate on -- on you based on your race, your -- your ethnicity.

GRAHAM: Would you be OK if -- if what Mr. MacTaggart said was

the law of the land, that when it came to behavioral advertising, you have to check with me?

HOFFMAN: I -- I think the biggest problem is that that puts too

big of a burden on the individual. What we need is a model that's risk based and puts the right controls on third-party transfer, the data brokers. I think that's the biggest concern we have.

GRAHAM: Or should we -- should we outlaw behavioral

advertising?

HOFFMAN: No, I think lots of behavioral advertising are things

that actually the individual would like to get.

GRAHAM: Mr. Weinberg, where's your view of all this?

WEINBERG: I think consumers need an easy mechanism to opt-out.

Mr. MacTaggart mentioned Do Not Track, I think that was a great...

GRAHAM: Do you agree with that, Mr. Hoffman?

HOFFMAN: I believe providing an opportunity to opt-out is -- is

critical, it's just the number of situations are going to be where individuals, that's too much of a burden to put on them.

GRAHAM: OK. Go ahead, Mr. Weinberg, because if you can convince

me, you can convince anybody, so I'm your perfect test case.

WEINBERG: Well, Mr. MacTaggart mentioned a decade-long effort

called Do Not Track which would enable consumers to be able to opt-out of behavioral advertising very easily.

GRAHAM: OK.

WEINBERG: By my estimations, 75 million people have it turned

on in their browser, 75 million Americans. And yet it's completely voluntary and does next to nothing.

GRAHAM: So you'd have to improve upon that, Mr. MacTaggart?

MACTAGGART: So what -- what will happen under CCPA is we've

already talked to browser companies. They'll put a setting in their browser. Once -- you set it once, and you set it and forget it. You just say indicate to everybody don't sell my information, then it's the law. It's not voluntary anymore.

GRAHAM: Right.

MACTAGGART: It's a huge impact.

GRAHAM: So my last question, how many of you believe the

federal government should preempt states in this area?

DEVRIES: Without lowering the protections that have been

established for residents in California and others, I think that a -- a federal law that sets out a comprehensive and consistent standard is the -- is the right thing for us to consider.

MACTAGGART: You know, I think the example with HIPAA, which is

the health legislation and GLBA which is the financial administration, that...

GRAHAM: Do you agree with his answer. He's saying using your

law as sort of the floor.

MACTAGGART: If it were a floor, not a ceiling, yes.

GRAHAM: Mr. Hoffman?

HOFFMAN: Yes, stronger and better law.

WEINBERG: No, not at this time. In theory, yes, but would like

to see the actual law.

GRAHAM: OK.

LEE: We think that strong reform is necessary and that

decreasing the overall regulatory burden.

GRAHAM: But making it a floor is OK with you?

LEE: Yes.

GRAHAM: Thank you.

FEINSTEIN: Thanks, Mr. Chairman.

First of all, let me just say something. I think this is the first panel in a quarter of a century that's I've been on that has complied with the time agreement. And so my congratulations...

GRAHAM: Then we're due. Then we're due.

FEINSTEIN: My congratulations to all of you. I'm still on

opt-in versus optee -- out -- opt-out. It's my understanding that all 28 of the European nations use opt-in. Why do you suppose they do opt-in?

DEVRIES: Thank you, Senator. The GDPR, it does require opt-in

for certain data processing, but not for all. And in fact, the GDPR contains an important concept called legitimate interests balancing.

So it says that if you believe as a -- as an entity that processes people's personal information that the legitimate interests that you've got in terms of what you're trying to offer to the user, the value you're trying to derive from that data balances well against the rights and interests of the user, that you can provide them a right to object, what we can an opt-out.

You could provide them that right as opposed to resorting to the express consent which is a very high-bar under the GDPR and they reserve it for that kind of processing activity that would require it.

FEINSTEIN: It -- I'll go down the line, but maybe you could

include -- I mean I'm not the most computer sophisticated person, but I like to know what I'm doing. I would like my privacy to be protected, and it seems to me that if somebody has a proposal, I should be able to say yes or no. And the way these notices go out, they're so small and such fine print that most people can't read them anyway.

So I think that the way one would know that they're protected is that they have to be able to opt-in as opposed to opt-out. And I'm really concerned about that. California's opt-out, Europe -- Europe is opt-in. So you've got an opt-in standard if you're a company that that's relevant to in at least 28 countries. Can you respond to that?

MACTAGGART: Yeah, one of the issues with opt-in is once they

get your permission, it's sort of business as usual. The consumer wants to use this service. There's a real -- real risk that the consumer is going to want to use the -- the services it's heard of, but the services it hasn't heard of, it won't give them permission.

So the new startup -- first of all, Europe doesn't have a minimum threshold. We have $25 million. But it's -- there's an innovation impact on the new startup, but the other thing is, so you're going to Uber. Uber kind of does need to know your credit card information. It does need to know where you're going.

FEINSTEIN: Speak a little slower (inaudible).

MACTAGGART: Sorry. So if you're going to a -- a site like Uber

where you're renting a, you know, getting a rideshare car, they do need to know where you're going. They do need your credit card information. They do need your name. So you're going to say yes because otherwise the service doesn't work. And the worry with opt-in is that this sort of a take-it-or-leave-it approach, it's -- it's either -- either opt-in or you can't use the service.

FEINSTEIN: But I could see the opt-out notice, you -- you know

you'd have to read it with a magnifying glass.

MACTAGGART: No. What we're -- what our law requires is on every

page that collects information, there's a button that says do not sell my information. You click it, and you just click it once. That's it.

And then in addition, just to make it even easier, we've already talked to the browser companies. As I was saying the browser companies will have a setting. You say I want to always not sell my information. You click that once in your browser, then every site you go to, you don't have to worry about it. It does it for you. That's the beauty of this. That's what the building (ph) of the Do Not Track is.

So you do it once, and then you have really meaningful -- something's happened in your life, you've now told all these companies don't sell my information. Whereas, in Europe, if you say, yes, you can process my information, then it's business as usual. Nothing's changed. That's the -- that's the distinction.

FEINSTEIN: Anyone else have a point of view on this? This is

sort of fundamental to me, so I appreciate it.

HOFFMAN: Absolutely. I -- I -- I think what's absolutely

critical in a model is to provide for situations where individuals can provide meaningful and practicable consent. The situation we have though, is that people don't read privacy policies now, and we're moving into an environment where there's going to be even more data collection putting the burden on the individual to have to consent to every situation where information is going to be collected from them.

And where we don't cover the fact that what is going to happen with technology is that more and more data about us is not going to be collected directly from us. It's going to be scraped from what other people put up on the internet. It's going to be taken from government records. We need protections that are going to cover that also. We can't put all of this burden on the individual.

Yes, we need to have mechanisms in whatever law there is to encourage companies and situations like Mr. MacTaggart was mentioning to ask people for their consent. But we need to cover these other situations also because that's where technology's headed. Intel's model does that by focusing on making it illegal to use data in ways that are going to harm people.

FEINSTEIN: Could they, just the two...

GRAHAM: Yes, ma'am.

FEINSTEIN: ... just quickly make a response?

WEINBERG: Yeah, quickly. As Mr. MacTaggart mentioned, a lot of

this easy opt-out is already built into the browsers. If it was mandated, then people would easily have an ability to opt-out of behavioral advertising, and then they wouldn't have to worry about reading all these policies (inaudible)...

FEINSTEIN: What happens in Europe then?

WEINBERG: In Europe, I would also hope that ultimately, they

respect Do Not Track in the browsers which is a worldwide setting.

FEINSTEIN: But now they do not? Now it's...

WEINBERG: Right -- right now hardly any company in the world

respects Do Not Track in the browser.

LEE: Echoing some of the comments you've heard, opt-in doesn't

escape the problem of mountains of fine print. We've -- we can see the implementation and what it

looks like when we look at sites that are compliant with GDPR. It standardizes the language to some extent, but it still put that burden of making a decision and parsing these legal agreements on each individual user.

So we think that while opt-in might be appropriate in some circumstances where there's particularly sensitive data or relationships between the entities, opt-out with rules of the road that make sense and are predictable and reliable is a better user experience and probably...

FEINSTEIN: Thank you.

LEE: ... a better way to go.

FEINSTEIN: Thank you. That's helpful.

Thank you, Mr. Chairman.

GRAHAM: Senator Hawley.

HAWLEY: Thank you, Mr. Chairman.

I'd like to start by noting that yesterday I sent a letter to the FTC Chairman Simons demanding that the FTC focus on enforcing our consumer protection laws, and with consent, Mr. Chairman, I'd like to ask that that letter be entered into the record.

GRAHAM: Without objection.

HAWLEY: Thank you very much.

I -- I'm concerned about the implicit bargain that consumers are being asked to ratify by which they get supposedly free services but actually had enormous amounts of personal data extracted from them without knowing what exactly is going on.

And, Mr. DeVries, I'd like to focus on -- begin at least with you and -- and your company, the largest arguably, the most powerful company in the world. I note in your testimony, your written testimony, you say for over 20 years now our flagship products have been free. And then you go on to say next paragraph that Google clearly explains how it makes money and clearly explains how your products use personal information.

And my question is is that really true? Are any of those statements actually true? So let's -- let's take some examples. Let's start with location tracking. Let's start with your Android phones. Do you think the average consumer would be surprised to learn that her location is recorded and sent to Google hundreds of times every day even when she is not using her phone?

DEVRIES: Thank you, Senator. I -- I do think we -- we take as

strong an effort as possible to try to explain these things clearly. I understand that it's -- it's complicated. The way a mobile phone works...

HAWLEY: But do you think that she would -- do you think she

would be surprised to learn that even when she's not using the phone, an Android phone, Google is receiving information about where she is -- for instance, it's every four minutes or 14 times an hour. Roughly 340 times during a 24 hour period. That's without using the phone. Do you think she'd be surprised to learn that?

DEVRIES: So, Senator, I -- I know that location information is

absolutely core to making a mobile phone work the way that you want it to work. It makes -- it's what makes maps work, it's what makes your phone calls be able to be routed correctly. And we have an optional service that's opt-in called location history which can collect location over time if people turn that on. I think there's more that we can do to explain location more clearly, and I've -- I've heard your concerns (inaudible)...

HAWLEY: Well, you -- you collect -- Google collects geolocation

data even if location history is turned off, correct?

DEVRIES: Yes, Senator, it can in order to operate other

services (inaudible)...

HAWLEY: Let's just -- let's just get that on the record. Google

collects geolocation history and information even if location history is turned off. Do you think that an average consumer, let's say a teenager with an Android phone would be surprised to learn that Google is tracking his location even when location services are turned off -- turned off by scanning Wi-Fi networks around him throughout the day? Do you think he'd be surprised by that?

DEVRIES: Senator, I know that this data is used to provide

value back to the user to make their phone work...

HAWLEY: You're not really answering my questions. Do you --

you're telling me you don't think a consumer should be surprised? You think they should anticipate that? They have location services turned off.

GRAHAM (?): This is fascinating. What value are you talking about?

DEVRIES: Well, Senator, so in order to make, say, maps work, to

be able to locate you to give you directions where you go, maps needs to know where you are.

GRAHAM: The phone's off.

DEVRIES: Well, in order to be able to just perform basic

functions to keep it (inaudible)...

HAWLEY: Location services are off.

DEVRIES: I -- indeed, Senator, in order to be able to know what

-- where it is so it can route phone calls to you, so it can collect the basic information.

HAWLEY: So the consumer cannot meaningful opt-out. I mean he

has...

DEVRIES: Sir (ph)...

HAWLEY: ... gone and tried to turn location services off, he's

not using his phone. It's still communicating and sending information to you, and you're monetizing it and using it to direct ads him, correct?

DEVRIES: We are not using that information to direct ads at

him, no, sir. This is to provide value back to the user in terms of making their services operate.

HAWLEY: What -- you -- what -- wait, wait, wait. You don't use

the information? What do you do with that information?

DEVRIES: We use it to make sure that the -- the -- we

understand...

HAWLEY: It's not a monetary value to you?

DEVRIES: There is some ways that location can be used for ads,

so for instance your IP address.

HAWLEY: Well, I thought you just said it wasn't used for ads?

DEVRIES: Senator, there is -- there is -- there is the -- the

kind of geolocation that's sent from the cell tower from your GPS device that's used for purposes that are really about making the phone operate. I'm happy to explain this in more detail. I understand it's a complicated topic and we can communicate it better and (inaudible)...

HAWLEY: I -- I don't know that it is that complicated. I think

when somebody turns off their user information, their location history, they expect the location tracking to be off. But it's not in fact. They don't have a way, apparently, to turn it off.

Let's take another example. Do you think that an average consumer who's using your products fully understands that Google builds a profile about her, tracks where she goes to work? Tracks where

her boyfriend lives. Tracks where she goes to church. Tracks when she goes to the doctor. Do you think that an average consumer would anticipate that?

DEVRIES: Senator, I -- I know that we have a duty to

communicate this information clearly. I don't believe we track the information to that level without communicating to...

HAWLEY: Do you think you're communicating it clearly when a

consumer cannot turn off their location tracking?

DEVRIES: Senator, you can turn off location tracking. There are

aspects of location, though, that are necessary to make services work where if we turn those off, your phone wouldn't work the way you'd expect. And I know that's a complicated subject to explain, it is and we're trying hard and we are (inaudible)...

HAWLEY: No, it's actually -- it's not complicated. What's

complicated is you don't allow consumers to stop your tracking of them. You tell them that you do. You would anticipate that they do. A consumer would have a reasonable expectation based on what you've told them that they're not being tracked, but in fact you're still tracking it. You're still gathering the information, and you're still using it.

By the way, all of this is just phone. We're not even talking yet about search or -- or internet tracking. I mean, listen, my time is almost expired here. We could talk about the -- the internet tracking that Google performs. We could talk about the lack of consent.

Here is my basic concern is that Americans have not signed up for this. They think that the products that you're offering them are free. They're not free. They think that they can opt-out of the -- of the tracking that you're performing. They can't meaningfully opt-out.

It's kind of like that -- that old Eagle's song, you know, "You can check out anytime you like but you can never leave." That's kind of what it's like dealing with your company. And that's a problem for the American consumer. It's a real problem.

And for somebody who has two small kids at home, the idea that your company and others like it are sweeping up information to build a user profile on them that will track every step, every movement and monetize that, and they can't do anything about it, and I can't do anything about it. That's a big problem that this Congress needs to address.

Thank you, Mr. Chairman.

GRAHAM: Senator Durbin.

DURBIN: Senator Hawley, you should come up to Chicago, or

perhaps we should invite here a group called Adelson (ph).

About six weeks ago, I sat down and they did a presentation along the lines you just mentioned. They also track how you move from place to place. Are you walking? Are you running? Are you on a bicycle? Are you in a car? So the information that is being gathered going way beyond what anybody imagines when they carry one of these around every single day.

There's so many aspects of this that I want to get into, but the one that troubled me the most is they said the largest collector now of information, and they can hardly keep up with the volume, is a collector of information on kids, our children. So it isn't a question of opting in or opting out personally. It's how much they're collecting on our children.

And a company known as Knewton, K-N-E-W-T-O-N, is collecting students', not only their grades so they can process a -- a report card. They're collecting their homework. They're collecting the essays they turned in. They are making a file on each of our children. So when a college announces we're no longer going to use the SAT and the ACT, it's because they don't have to. They already have the information.

Listen to what Mr. Jose Ferreira, CEO of Knewton said in 2012. "You can look at some students and think, boy, that poor schmuck is really in a lot of trouble in school." They've already branded the kids. That information is there.

So the question I really raised and introduced legislation to deal with it, can kids opt-out at a later point in their life? Can they ask if all the information that's been accumulated about them before the age 13 be wiped clean? Is that a reasonable request? I ask anybody on the panel.

Mr. Hoffman?

HOFFMAN: I -- I would say, and Intel's model does this, that we

need to provide the ability for people later in to say -- to come back and say, look, not just the type of information that was collected from me, but now how analytics are applying to it to be used in ways that could harm me, this is disproportionate and I should have the ability to have that data either obscured or deleted. And that's part of the Intel model of this specific language for the bill that we proposed.

DURBIN: So here's the problem, when Mr. Zuckerberg came and

subjected himself to 42 senators asking questions, I asked him a couple questions. "What's the name of the hotel you stayed in last night?" And he said, "I really don't want to tell you." I said, "Well, tell me who you've communicated with in the last two days on your phone?" "I really don't want to tell you." So he -- he obviously valued privacy.

Then we asked him about Facebook Messenger and he said in general, that data is not going to be shared with third-parties. Mother, father, is that good enough in general that won't be shared with third parties?

So what we need to do is to basically say it definitely won't be shared with third parties, and it can be deleted by a child after they reach the age of 14 and beyond. Is there anybody here who thinks that's an unreasonable idea to protect our children from having the information about their lives become part of the public domain, or at least the domain of those who want to use it for business purposes? Any problems?

MACTAGGART: Sir, not only is not unreasonable. It's totally

reasonable. But I actually think it should be all of us. I mean all of us should have these rights. And -- and -- and until 10 years ago...

DURBIN: Whoa, whoa, whoa.

MACTAGGART: Sir (ph).

DURBIN: All of your companies should have the rights?

MACTAGGART: All Americans.

DURBIN: I see.

MACTAGGART: Sorry (ph).

DURBIN: OK.

MACTAGGART: Yeah, and -- this is a relatively recent

development, this behavioral advertising. And for -- for -- for most of, you know, ad tech's history, it's been the contextual stuff. You're -- you're reading an article on pickups, you see the ads for the Fords, and no one cares about that. This -- this ability to track you and start to kind of guess who you are and what you're going to be doing even before you know it. That's...

DURBIN: The folks at Adelson went so far as to show the aerial

photographs of their homes which could be easily determined, the information Senator Hawley asked earlier about location and such. So their homes were now in the -- in the domain of those who wanted to decide how to advertise to -- when it comes to their whereabouts.

Let me ask you about the actual disclosures online. How many of you have ever read one of those? Oh, well, you're -- going to disqualify you. I would just say that basically none of us do. And if we tried to, we couldn't understand, right? And that is where you are opting out and opting in when it comes to your personal privacy. So shouldn't the burden be on you and your companies and say we are out until you make us come in? Isn't that really (inaudible)...

MACTAGGART: Well, that's exactly why we have the opt-out which

we think is going to be automatic. Set it -- I wanted to never have to read another privacy policy in my life. I want no one to have read them. We give the same right to everybody. You click it once in your browser, you're done. Your -- your information's never sold again. That I think is a really important right to give Americans?

DURBIN: Well, I -- I hope that's the standard.

Mr. Weinberg, I went to my phone here and obviously compromised my privacy, and decided to look at DuckDuckGo and the first thing I find is -- is to install your service. I have to go to Google Chrome. Aren't you sleeping with the enemy?

WEINBERG: You mean the Play Store? You have to use the app

store?

DURBIN: Yeah.

WEINBERG: Yeah, unfortunately, that's the only way to install

an app on an Android device.

DURBIN: I see.

WEINBERG: That's easy to use.

DURBIN: Well, I -- I want to tell you that your model sounds

like what I think America should look like. Thank you.

WEINBERG: Thank you, Senator.

BLACKBURN: The gentleman's time has expired.

Senator Kennedy for five minutes.

KENNEDY: Thank you, Madam Chairman.

Good morning, gentleman. I may have to interrupt you -- some of your answers. I'm not being rude. I'm just trying to get through my questions. And I would appreciate it if you'd speak English to me.

I -- I think we can all agree that the digital promised land has a few mines in it. I think we can agree that social media can now influence what we believe, how we vote, what we buy. Even how we feel.

I want to start with Mr. DeVries with -- did I say that correctly, with Google? Congratulations on your success. You're -- you're no longer a company, you're a country. How long is your -- how long is Google's user agreement? How many words?

DEVRIES: Sir, the -- our -- our terms of use, the user

agreement, I -- I don't know off hand. The privacy policy which is what I focus on...

KENNEDY: How many -- how many pages is it?

DEVRIES: Our terms of use, I don't know. It's -- it's certainly

got a lot of words in it. My privacy policy, which we work on, which describes how we use this (ph) information.

KENNEDY: I -- I looked at your user agreement. I eyeballed it.

Figuring six characters per word, it's about 3,600 words. That's about seven pages single-spaced. You could hide a dead body in there and nobody'd ever find it. How -- how many -- you -- you can track people, how many of your users read it?

DEVRIES: Sir, we have millions of users who come to our privacy

policy.

KENNEDY: Right. And how many of the read it?

DEVRIES: Well, I -- I can't say that very many, I'm sure, get

all the way through it. I know it's not the top of people's reading list. But...

KENNEDY: I mean you can -- I'm not trying to be rude, but you

can track everything else. Have you ever tracked that?

DEVRIES: We certainly try to keep track of how many visits we

get to our privacy policy. But we -- we would have no way of knowing if people actually read it, and we do our best to make it comprehensive.

KENNEDY: Well, how many people -- how many people as a

percentage of your total users go and -- and click on your privacy policy or your user agreement?

DEVRIES: Well, we have visits to the -- the account page which

is where the privacy policy is. We actually have...

KENNEDY: Just give me a number if you could.

DEVRIES: We have 2 billion users a year (inaudible)...

KENNEDY: How many click on the user agreement? Do you know?

DEVRIES: Far less. In the millions, but far less than that.

KENNEDY: OK. Can you connect my data that Google has on me to

my name? Not do you do it. Do you have the ability to do it?

DEVRIES: Senator, if you have a Google account, it allows you

to put your name in, we would collect it there. If you don't, we cannot.

KENNEDY: Can you connect my name to my data. I'd really be

grateful if you would answer my question.

DEVRIES: Senator, if you have a Google account we can, if you

do not have a Google account, we cannot.

KENNEDY: OK. So, you can put a name to my data?

DEVRIES: Well, that's -- that's the way people use Google. They

-- they, you know, they send e-mail with Gmail, et cetera.

KENNEDY: Yeah but you -- you have the ability to put in, let's

say John Neely Kennedy, and find everything you want about me in terms of my data. What websites I go to, what ads I read, what I buy, that sort of thing?

DEVRIES: Yeah. And -- and we try to show that to you, Senator.

KENNEDY: You -- you do that?

DEVRIES: If you have a Google account, we do that. And we

provide you that information. You can see that, and you can delete it.

KENNEDY: So, you do that repeatedly? I could call you up and

say, give me all the information that you have on Thom Tillis, and I'll give you a quarter of a million dollars, you can do that?

DEVRIES: Senator, we never sell our users personal information,

we wouldn't do that.

KENNEDY: Can you do that?

DEVRIES: We would never do that. This violates our...

KENNEDY: Can you do that?

DEVRIES: Not legally, no.

KENNEDY: Could you do it, technically?

DEVRIES: Well, yes, sir.

KENNEDY: OK. I think -- I think -- well, strike that. Is there

any -- is there any type or piece of data that Google would not monetize?

DEVRIES: Oh, yes, sir. We -- we -- most of the data we collect,

we don't actually use for advertising purposes. We use it to provide the services back and try to make them better and work better for users.

KENNEDY: All right. You already have to comply with the rules

promulgated by the E.U.. Do you not?

DEVRIES: That's right. It's been like that (ph)...

KENNEDY: And by California. Do you not?

DEVRIES: The California Law has yet to go into effect but when

(inaudible)...

KENNEDY: When it does, you'll have to comply?

DEVRIES: That's right.

KENNEDY: That's a lot of people. What's the problem with just

extending that to everybody else?

DEVRIES: I'm sorry, extending? Oh, the California rules to...

KENNEDY: And the E.U. rules.

DEVRIES: Well, certainly. And we apply, aside from the rights

that only apply specifically under European standards, we apply...

KENNEDY: Would you object to just -- since you have to do it

there, just doing it for everybody?

DEVRIES: No, that's not our objection to having a lot of stuff

(ph)...

KENNEDY: Would you object?

DEVRIES: Well...

KENNEDY: Answer my question, Mr. DeVries. Would you object?

DEVRIES: We certainly would extend rights that we have to

(inaudible)...

KENNEDY: Would you object?

(UNKNOWN): (Inaudible).

DEVRIES: We would not object to offering people rights

(inaudible)...

KENNEDY: All right. Thank you -- Thank you, Mr. DeVries.

BLACKBURN: Gentleman yields back.

Mr. Coons, five minutes. Chris?

COONS: Thank you Madam Chair and Ranking Member. Thank you to

our witnesses. I think it is really important, that we have a thorough and open conversation about privacy and legislation. This is something Senator Flake and I started last year with a series of roundtables with advocates, industry representatives, folks from all over our country.

At the heart of this debate is a cost benefit analysis that I -- I think it's just not clear to most consumers. Social media users, like myself, benefit immensely from being able to use the platform, share information with friends, neighbors, family, constituents. And then social media companies like Facebook, or Google, or others benefit by using data to sell ads targeted to me based on information I share.

Normally, that interaction is great because I'm able to reach friends and family without paying a fee and Facebook and others are able to grow their business. But there are huge risks as has been detailed by many on the panel and by many here on the committee. Digital advertising companies might not unlawfully target individuals based on protected class such as race, and data that they generate and create around health care, or other protected proxy issues.

But the use of predictive profiles in order to target certain groups with ads for things like housing, employment, banking, and education have significant consequences that I don't believe the average American has really thought through. And the consequences of our legislating will be significant. We have to find a way to both significantly increase data privacy protection and clarity, while not destroying the opportunity for competitiveness and innovation that has led several of the largest companies in the world in this space to be American.

So, let me just first if I could to Mr. MacTaggart, do you think the average consumer, the average American consumer, appreciates how data can be utilized to affect their access to get a loan, to find a place to live, their access to higher education, the ways in which behavioral predictive advertising can really narrow their range of options?

MACTAGGART: No. I think the average person has no idea.

COONS: And do you think the FTC could employee it's unfairness

authority under Section 5 of the FTC act to address these secondary and discriminatory impacts of data collection and targeted advertising?

MACTAGGART: Sir, I'm not an FTC expert but I think there -- the

-- I think that's a -- what I've heard from those who are is that they would like more tools to be able to address this issue.

COONS: Mr. Hoffman, I think you worked at the FTC before your

current role at Intel, if I'm not mistaken.

HOFFMAN: I -- I did not. I've worked with the FTC for

(inaudible)...

COONS: With the FTC as an outside advisory, right?

HOFFMAN: That's right.

COONS: Forgive me. The FTC already has some authorities to

regulate and protect consumers privacy, but I'm concerned they're not doing enough, and they need greater resources and great authorities. Are there any recent examples you could site or would anyone else like to offer this, of the FTC utilizing its current authority under Section 5, and then what risks to consumers remain outside their authority that we should address?

HOFFMAN: I'd like to take the second half of your question, if

you don't mind, which I -- I would say first that not all industry sectors are actually governed by...

(UNKNOWN): Right.

HOFFMAN: ... the FTC which is a significant issue. The FTC

doesn't have role making authority, which we think would be absolutely critical within certain statutory guardrails so that it's narrowly prescribed. And we also think that the FTC absolutely needs civil finding authority.

COONS: Is one of the most important enforcement aspects, Mr.

MacTaggart, of CCPA the private right of action?

MACTAGGART: So, the private right of action only applies to

negligent data breach. The rest of it is enforced by the Attorney General, and we did give the Attorney General rule writing authority because precisely we thought, this is a fast-moving area, we didn't want them to have to come back to legislature every time. So, at one level, this is -- CCPA is a framework to give -- to set up a privacy regulator in the office of a Attorney General and give them the -- the ability to -- to regulate a very fast moving area of the economy.

COONS: Mr. DeVries, you just had an interesting exchange with

Senator Hawley. I am too am concerned about Google's data collection. There are about 2 billion mobile devices running on Android. There's cookies all over the internet, there's lots of different ways that data's collected. One way Google uses this data is to profile consumers for targeting ads. Do you have a specific profile that is identifiable for every user?

DEVRIES: No, Senator. We have a profile that could be related

to your Google account if you have a Google account. You can see that profile, you can delete it if you want to. And if you want to, even if you don't have a Google account, and you just had a -- a cookie that we might use to -- to target ads, you can opt-out of that, or you can delete your cookies.

COONS: Let me ask a different way. Is there a way, just to

rephrase this issue, is there a way to use an Android device and other Google products without having Google collect data on a consumer's interaction with that product? Because I've seen information that persuades me that's not true. That Android continues to collect data on you even with the SIM card out, even with the privacy protections all turned on.

DEVRIES: Thank you, Senator. There are ways to turn off all of

the use of your data for advertising. Some data needs to be collected to operate the service. To make sure the service is working, it's secure, and make sure and make sure your battery life is -- is healthy on your phone so it doesn't run out faster. Those kind of functions with continue. But the use of your data for advertising can be completely disabled.

COONS: Thank you. I -- I would also be interested in the

portability that Mr. Lee and Mr. DeVries raised but I note I've exceeded my time.

Thank you, Madam Chair.

BLACKBURN: Gentleman yields back. I will yield myself five

minutes for questioning. I want to see a show of hands. How many of you believe that Americans have a right to privacy when they are in the virtual space, raise your hand? All of you do?

How many of you believe that should be a protected and constitutional right? Awesome. All of you do. OK. When we're talking about privacy, and that stands to the individual, do each of you agree, that your PII is your virtual you, and you online. Raise your hands.

OK, Mr. DeVries, you're a little slow on the uptake there. Do you have a disagreement with that?

DEVRIES: No, ma'am.

BLACKBURN: OK. Who owns the virtual you?

DEVRIES: Ma'am, your personal information is your information.

That's something that's according to my beliefs.

BLACKBURN: So, you would agree that the individual owns their

virtual presence online? Is there anybody on the panel that disagrees with that? You know, I find it so amazing as we have worked on this issue through the years. The issue of privacy, of data security, of intellectual property protection, that one of the things that is fascinating, is many of the tech companies or the FANGS. They have built their net worth off of individuals information.

And, Mr. DeVries, while you say you don't sell that information -- pardon me. Going back to Senator Kennedy's remark, basically, what you have done is coalesce that information. And that tracking and then you have built the essence -- the essence of that individual online. Do you agree with that?

DEVRIES: Senator, we do try hard for the -- to in order to

provide value back to the user, to understand...

BLACKBURN: You didn't answer.

DEVRIES: Yet...

BLACKBURN: Pardon me. You...

DEVRIES: Yes, (inaudible).

BLACKBURN: You -- you're not answering the question. Let me go

to this. On a Google operating system, on the Android phones, we'll go back to Senator Hawley's question. I have seen these phones and I will -- I want you to tell me if this is correct or not.

If you take that Android mobile device, and you pull the SIM card, and that device is turned off, then when you turn that phone back on, it will download every single base station that you have passed. That the tracking is embedded in the hardware, and it is always tracking you. And there is no way for that device to not be tracking you.

And Senator Durbin even mentioned. It will tell you if you're walking, or if you're riding, if you're in a building based on the barometric pressure, it will tell you what floor you're on, and what side of the building you're on. Is that correct?

DEVRIES: Yes, Senator, I understand there's lots of

(inaudible)...

BLACKBURN: That is correct. OK. I think that's fascinating. And

see most Americans would not -- would not see that as being information that you are entitled to. Because going back to what Senator Kennedy said, then you are saying you own the virtual you. Would you not agree with that?

DEVRIES: No, Senator, that's not how I conceive of it.

BLACKBURN: You wouldn't agree with that. Then that is amazing

to me. You could know everything about somebody and everywhere they go, and you hold that information. And the individual doesn't hold it. Let's move on to what you're doing with Chromebooks, and the operating system there.

Now, the reason SAT's are not as relevant, is probably because what you all are doing when those children are doing those assignments online, you're recording all of that. Is that not correct? And then you're also looking at the sites they go to and using that to maybe not put ads back on that laptop that is in the school but selling that to advertisers of the parents that are in that community. Is that correct?

DEVRIES: No, ma'am. We do not use any of the data that we

collect via these education products that we offer...

BLACKBURN: How do you build a profile on the students?

DEVRIES: We don't try to build a profile on them.

BLACKBURN: You don't?

Mr. Hoffman, how do they build that profile on those students?

HOFFMAN: I -- I'm not an expert on their services and how --

and how their products operate.

BLACKBURN: OK. Thank you, I appreciate that. How many of you

support having congressionally passed privacy legislation? Raise your hands. All of you do. How many of you think that we should give the FTC the authority to oversee you and to put rules of the road in place, to allow people to choose to opt-in, rather than assuming it is going to be an opt-out. How many of you favor that? No one favors giving consumers the ability to opt-in?

HOFFMAN: I favor the -- the -- the ability for consumers to

provide an opt-in I just believe that the regulation needs to go behind that because it's necessarily but not sufficient.

BLACKBURN: OK. I appreciate that. My time is expired but I will

tell you. I think the reason you do not want to have opt-in, is because it would change your business model. And it would diminish your profits. Yield back.

Ms. Klobuchar, you're recognized now.

KLOBUCHAR: Thank you very much, Madam Chair. Thank you to all

of you for being here today. This is a very important matter and we actually just had recently at a hearing on this in the Commerce Committee, and there, there was a lot of tears shed about all this patch work Mr. MacTaggart of bills across the country and I made the point well, the reason this is happening is because of the companies have been lobbying against privacy legislation for years and nothing has happened in Congress.

And Senator Kennedy and I have a bill, while (ph) not perfect, it's a bipartisan bill, that it has a number of provision in there including notice of breach. But we don't have preemption in that bill. Simply because I think we should allow states to also do their own thing. But if we get a very strong bill, maybe that would look differently. But I don't -- I don't think we're there yet.

So, could you talk about the important of notice of breach and also why you think opt-out is so important.

MACTAGGART: Well, first of all I think notice of breach is --

is essential because otherwise you just would never know. And so, you know, in our law, we -- we do (inaudible) but around negligent data breach. And what we said basically is look, if you encrypt your data, if you redact the data, or if you have reasonable practices and procedures in place to protect the data, there's no liability.

Why we didn't want to have a situation where the Russian government, you know, hacks in to a company that's trying to do its best and then all of a sudden, they have a big -- big liability. But if the company doesn't encrypt, they have a problem. And then we went out -- opt-out again because I think that that's the most effective way of giving consumers the best level of privacy. I think the problem with opt-in is it gives a false sense of -- of -- of security.

KLOBUCHAR: OK. One of the things, I was in Austin this weekend,

at South by Southwest and few policy proposals were made there but I brought up this idea of kind of getting at what some of my colleagues are talking about how the individual consumer is monetized, basically. Like they are a pry (ph), they are a commodity to many companies.

And so, one idea would be for these -- you could do it with large platforms, you could it with large amounts of data, but that some kind of tax be placed on them, not on the consumer when they use that data or transfer that data and then that money could go back to the consumers or it could go back for cyber-security for our country. And could you talk about that? I know there's something similar being discussed in California.

MACTAGGART: Yeah. The governor recently mentioned the proposal

about data dividend. I think, you know, the only thing would be to say, I think transparency is the most important thing. And to feel like consumers understand, I think the -- the worst outcome is -- would be a relatively tiny amount of money going to people and then there's all this behavior that we're trying to address right now that gets (inaudible) forever.

KLOBUCHAR: Right. Well, this wouldn't be on its own. This would

be in -- if you don't have privacy legislation...

MACTAGGART: Sure.

KLOBUCHAR: ... it doesn't really matter. This would be for when

they do do it, in a perfect world, where you have permission and you're doing it and then you get something out of it.

I don't know if you want to add anything, Mr. Weinberg, on this front.

WEINBERG: Not specifically. But as it relates to weakening the

data monopoly at the core of the advertising market, I think all options should be on the table.

KLOBUCHAR: Right. Thank you, that's a very nice way to put it.

Mr. DeVries, the Honest Ads Act is something that I've been fighting for more rules of the road for political advertising, which as you know, billions of dollars collecting data, selling ads, and the Honest Ads Act is a bill that actually has gained I think 12 republicans now in the house and it simply says that for ads that are political in nature, that it has a disclaimer of who's paying for them so you know who's paying for them and then it's disclosed.

And in fact, that's what you do for newspaper, TV, and radio, but we have billions of dollars spent online on political ads. Last September, Google announced its support of the bill and do you agree that we need to be consistent and will you pledge to continue to work with us to get this bill done?

DEVRIES: Thank you, Senator. And thanks for your leadership on

this. Ad labeling is not an issue I have a lot of direct knowledge on, but I understand that we're supportive of the goals to your bill and would love to work with your office on it.

KLOBUCHAR: OK. Anyone else have a comment on that because the

elections are coming up and we still have no rules of the road in place for issue ads most importantly as well as candidate ads.

MACTAGGART: Yeah, Senator, the one thing I would add here is,

you know, I -- I got concerned about this during the campaign and I had my attorney look into it and produce a memo. The real issue is not with the ads, it's with the fact that if you don't coordinate with campaign, and you don't expressly advocate for the election or -- of a senator or of a political representative, that's the first amendment right of the corporation to influence elections.

What you actually can do legally, with no disclosure, is you can up or down rank a -- a story about a politician. You can up or down rank a (inaudible)...

KLOBUCHAR: I understand all that. That is another issue but

what we have here, were ads that were bought by, in rubles...

MACTAGGART: Yup.

KLOBUCHAR: ... by Russia. We have issue ads that are meant to

disrupt that we don't even know who's paying for them and now we have some sites voluntarily archiving them and disclosing, but they're just going to gravitate to the sites that aren't. And that's just going to keep happening unless we pass some rules around.

$1.4 billion was spent online on these ads and it's going to go up to $3 to $4 billion in the 2020 election. And it's outrageous to me that we have no rules of the road in place. And I will have some questions about the FTC -- the FTC investigations that I'm supportive of on the record because I'm out of time. Thank you.

BLACKBURN: Senator Tillis, for five minutes.

TILLIS: Thank you, Chairman. Thank you all for being here. I

think that this weekend, I had a personal -- number one, I know all of the Google settings and there's not a whole lot of information you can get from me and I normally browse in incognito mode unless I want to be consulting on maybe some purchases that I'm making.

So, I think on that we need to do is understand -- there's a lot of good that comes from these tools. It's a matter of getting it right. I saved couple hundred dollars this weekend on some things that I was buying because A.I. suggested something I wasn't thinking about.

I think DuckDuckGo may have gotten me there as well, but it gave me alternatives that made me a more informed consumer. On the one hand, it seems creepy to think that any of these platforms, not just Google, there's a number that we could list, could know that you went to the doctor.

On the other hand, if we can figure out a way to protect consumer data, it may also be a trigger to make sure that that person after they went to the doctor, got their medications and followed their prescripted (ph) course for getting well.

So, the point here is getting this right. I for one thing that there has to be preemption. Because this larger complex -- the -- the merits of California are actually seem to be accepted by most of the people on the panel but who knows what other 50 or 60 or 80 different proposals could come into play. Maybe even get to the municipal level for data privacy. That makes no sense at all when we're talking about competing in a global environment, so we've got to get it right.

Mr. DeVries, I think that -- it is DeVries, right? Yeah. I think that one of the challenges that you're going to have moving forward is having people understand the difference between Android the technology stack and Google, the service that people are using.

Because I think what you were trying to say is as an operating environment for a phone, like iOS, you have to capture certain information for the phone to operate. Or you're simply not going to be able to -- be able to determine where you are and to actually link in to the wireless network.

So, I'd work a little bit on explaining your social media platforms and distinguishing that between the underlying operating environment that operates the phone. Like iOS, like Microsoft, for goodness sake. I mean, this is not just limited to phones. Any Chrome tablet or any Microsoft tablet or any other variant for an operating environment have these tracking mechanisms that can be good and bad.

I for one worry when I hear a committee hearing like this because I think that we could have a Dodd-Frank like overreach on fixing something that needs to be fixed. Every single one of you

should be good stewards of customer data. When there's a breach, it's on you. It's not he consumers problem to fix your problem to the extent that your platforms were breached. Got to work through all that.

But if we're not careful, we actually have this sort of populist reaction that at the end of the day, could be the debt to the detriment of the consumer. For those of us who want to use it, for those of us who are maybe informed enough to -- to be more protective than others. But I'm not naive, I know there's probably vulnerabilities that I -- that I experience.

Mr. Weinberg, I did download DuckDuckGo while you were doing your opening comment. And I don't know if it was Google Play or you all that did -- before I got to use DuckDuckGo, the first thing I got was an advertise for creepysite.com. And I'm going to look that up too. It looks like an interesting site to protect my customer data.

But I don't know -- I mean, the fact of the matter is, you're able to access me because Google Play has a platform that you can actually distribute your product. That's why we have to understand this ecosystem is more complicated than just jumping on a populous notion that you're somehow exploiting consumer data and that you should be stopped.

Because if you get stopped, then all of a sudden you got a credit card that you need to offer Google if you want a Gmail account. I mean you've got to -- you've got to -- these platform shave to derive revenue somehow. And right now, they're free platforms that have kinks that need to be worked out, protections that need to be improved, but we need to be very careful with respect to global competition and other challenges that we have if we overact.

I do believe that we need to preempt, I do believe the California law is better than I would have expected out of California to be honest with you, from my side of the aisle. We need to look at the European model and some of the problems that it has but we need to come up with well-reasoned policies that allow -- that do not create a new barrier for entry.

If you're operating in ten states, ten countries and the District of Columbia, you may have reached the scale to where you can deal with additional regulatory complexity, I want the next DuckDuckGo to be able to get in and not be at a point to where the regulatory burdens are too great.

I'm not here to ask any of you all questions. I would tell you all I'm glad to hear that generally speaking you think preemption is necessary, we should make sure that the most innovative nation in the history of this planet continues to be that. We need to make sure that global competitors could replace you all and not necessarily be held to the same standards. The risk of breach would be great.

So, we need to get this right and we need to make sure that we understand the technology stacks and all the various layers that go into getting the policy right. Thank you all for being here, it was very informative.

BLACKBURN: Senator Hirono, five minutes.

HIRONO: Thank you very much. I think that we're at a point

where I think there's recognition that we do need privacy legislations. So, it might be (ph) we should be focusing on what type or protections we should provide to consumers.

And I think one of the critical questions is whether the privacy regime is an opt-in or an opt-out. And there is significant evidence that privacy defaults are sticky, and consumers rarely alter their default privacy settings. Would you all agree that's the case?

Yeah. Once you are in there, they forget about it. So, this is why in my view, the privacy regime should be an opt-in. Because I think most of the default settings require an -- an affirmative opting out. So, an opt-in -- to require the consumer to -- to opt-in to getting all these ads et cetera, is much more protective of the consumer. So, let's just go right down the line. Would you support privacy legislation that uses an opt-in as opposed to an opt-out requirement?

DEVRIES: No, Senator. I don't think that's the right approach

across the board. Opt in is certainly the right place for the -- the most important choices, but I wouldn't want to overwhelm users by having opt-in for everything. It would -- I worry it would cause click fatigue. People would just start agreeing to everything as opposed to...

HIRONO: No, opt -- opt-in means -- so the opt-out would be --

here, let me -- let me make myself really clear. So, a consumer automatically opt-out of getting any of the ads et cetera. So, that I think it decreases the -- the desire on the part of Google et cetera to get the kind of information about us.

So, we would automatically be opted out of all of these (inaudible) ads et cetera, and we would have to affirmatively opt-in to have your start using information about us. That's what I mean. And I would like to know from each of you whether an opt -- to affirmative require opting in to get all this -- these ads is -- is something you would support.

DEVRIES: Thank you, Senator. I -- I think we have an experiment

under the GDPR with that exact rule. So, we can see how that works. It's certainly something to consider, but I don't personally support it, no.

HIRONO: Well, because it would really limit the uses that you

have for the personal information that you collect.

DEVRIES: For Google personally, we rely less on personalized

ads than on the contextual ads but for many of our customers, our publishers, and app developers, this is the significant or portion (ph) or majority of the revenue is targeted ads. And so, we're concerned about the ecosystem.

HIRONO: Sure. But in terms of protecting the consumer from

being tracked, and the use of the tracking information to buy advertisers, the consumer will be much better protected by simply having opt-out as the default.

So, for example, Google controls advertising on non-Google sites. And my information is that Google controls the advertising on 75 percent of the most popular websites. Is that not true? (Inaudible).

DEVRIES: I -- I don't know the number we certainly have a lot

of customers out there, yes.

HIRONO: It's a lot. Yeah, Google makes a lot of money. In fact,

Google had over $136 billion in revenues last year. That's more than a billion dollars a week. So, let's just go down the line. Mr. MacTaggart, would you support a regime that would -- would basically require consumers to opt-in to get all this advertising?

MACTAGGART: So -- so, what as I hear you, Senator, I think

you're describing a third way. Because the -- the one in Europe is opt-in or not. And once you've opted-in the companies can sell you data, so it's kind of business as usual.

And that's my worry. Is that you opt-in and then -- and then nothing really changes. Our -- our example is opt-out. I think what you're saying is if there were a default where you could still use the service but, we're already opted-out...

HIRONO: But what I'm saying is that the default setting would

be opt-out and I as a consumer would have to actually affirmatively consciously opt-in to the use of all my data for, heaven knows what.

MACTAGGART: Yeah, but the problem there is once you opt-in to

the service then it's business as usual. We...

HIRONO: But you always -- if one opts-in you should always have

an opt-out feature. But this one has to actually -- do you get what I'm saying?

MACTAGGART: I...

HIRONO: I feel like -- the -- I think the -- the -- the --

person from DuckDuck of the, you know, what I'm talking about. So, I would say for a consumer -- consumer protection having the default as opting-out, automatically opting-out on, as the consumer opts-in is much protective of our consumer's privacy. How about you, third...

HOFFMAN: As I mentioned before in the response to the FTC

question. There's going to be situations particularly for risky uses of data where opt-in is necessary. The problem with an overall either opt-in or opt-out approach is examples like I provided in my -- my opening statement with Donna, the victim of the -- of -- domestic violence.

Police officers, elected officials; the information didn't come directly from them. If we rely just on that type of a model protection increasingly where technology is going...

HIRONO: Well, if...

HOFFMAN: ... we're not going to protect them.

HIRONO: ... I just need to -- Madam Chairman, I just need to

hear from the other two gentlemen. There may be some instances where we need to provide certain -- I don't know, we, we'll have to figure that part out.

But Mr...

WEINBERG: Weinberg.

HIRONO: ... Weinberg.

WEINBERG: Yes, Senator. We would support that. Just would like

to also point out that Americans in large numbers have found they do not track setting in their browser by about 25 percent. And so, people are trying to find these settings.

HIRONO: Yes. It's not easy either to find those settings.

Mr. Lee?

LEE: Senator, I think you're right when you say the defaults

are sticky. But I also think Mr. MacTaggart's right that moving too far opt-in would create a take it or leave it approach. People would wind up opting-in agreeing to these exact same fine print contracts that no one actually parses.

HIRONO: I know, but most people will not make the decision to

opt-in. I can pretty much tell you that.

BLACKBURN: And the lady's time has expired.

HIRONO: Thank you very much.

BLACKBURN: Senator Whitehouse, five minutes.

WHITEHOUSE: Thank you, Madam Chair. Thank you all for being

here. I am finding small companies in my home state of Rhode Island that are subject to GDPR without knowing so. Because they have in our global economy a business link with the E.U. that makes them liable.

And I think probably the majority of companies that have that liability don't even know about it. So, I agree that we need to take some step to try to bring some conformity. So that they're not walking into invert liability under GDPR standards they didn't even know they were subject to.

Has anybody looked at the privacy shield program between Switzerland and the U.S. and if you have, is that a useful model for considering legislation going forward?

DEVRIES: We comply with the privacy. We use the -- the -- the

U.S. -- both the U.S. E.U. and the U.S. Switzerland agreements to be able to transfer data lawfully. So, we are familiar. That agreement is really focused on the idea of lawful transfer of data from those countries to the U.S. for processing.

WHITEHOUSE: Yeah.

DEVRIES: So, it's not complete as a privacy regime but, it

certainly, has -- gives a lot to offer, gives us a good starting place to look at.

WHITEHOUSE: OK. Let me raise a different point. One of you

mentioned earlier that at this point these big data companies -- might have been you, Mr. Weinberg. Now how more data on individuals then any security service has in the history of humankind.

And obviously, we have considerable concerns about so-called big government having enormous amounts of information on the public and what misuse that might be put to. The problem that I see right now is that the division between private and public. Between government and particularly certain big business that engage with government in a way that they actually want to own, control, and manipulate government on their behalf.

It puts us in a position where you can easily have these data services made available to government probably through a political party rather than through the actual government agency. But nevertheless, it becomes fully operative in our political space. We saw Cambridge Analytical try to do that. Succeed at doing it, get caught and blow up.

But I think more to come behind that and, I worry about how weak our defenses are in this area. When we had the hearing with Mr. Zuckerberg of Facebook, he sat in front us and said that their policy for finding who was launching political advertising on their -- for -- medium, was that they had to disclose the corporate name of the entity that placed the advertisement.

So, as simple a device as a, phony baloney, shell corporation completely defeats Facebook's effort. And that's so bad an effort that's it's hard to believe that they're actually sincere about trying to identify who is behind political ads. Because it's really not hard to set up a regime where you have to chase it through until there's a real company that's doing real business or a real person with a real human name.

And so, I remain very suspicious of the -- this being a particularly dangerous area in which data gets deployed for political purposes through government by potentially a political party rather than the government itself. But to the same effect.

And I wonder if any of you have a particular -- yes, Mr. MacTaggart?

MACTAGGART: Well, Senator, I think as I was saying earlier. The

issue -- is one thing you're talking about is -- is a foreign entity or another entity. But think about the entities themselves. It's a first amendment right of the corporation to -- as long as you're not in direct coordination with the campaign, it's legal, there's no disclosure.

They can up or down rank a story about you and your reelection. They can show more news or less news to a swing voter in your district, in an effort to influence. It's totally legal and there's no disclosure required. That's the part that's actually -- when you look at it in terms of a democracy, I mean, it's just a bomb sitting in the heart of the democracy...

WHITEHOUSE: Yup.

MACTAGGART: ... right here. And something needs to be done...

WHITEHOUSE: Maybe (inaudible) and waiting to be -- waiting to

go off. And I -- I think it's something that we need to pay attention to in this conversation. You agree?

MACTAGGART: Completely, agree.

WHITEHOUSE: Yes. OK. My time is up. Thank you all very much.

BLACKBURN: I thank the gentlemen for finishing with five

seconds to spare there.

Senator Blumenthal, five minutes.

BLUMENTHAL: Thanks, Madam Chairwoman. In case anybody had any

doubt, privacy is all the rage, bipartisan. But as frequently, happens the devil really is in the details. And my view is first, do no harm. We have a very profoundly significant advance in California.

The GDPR represents progress and what I see is lots of good intentions invoking privacy in the name of undercutting rather than advancing what we have now through the use of preemption.

And I am helping to lead a group in the commerce committee, as you may know. Involving a bipartisan core of support for adopting a law that regards California as a floor, not a ceiling, in terms of the privacy standards for both the expectations of what the standards should be but also enforcement. And so, I really feel strongly that we should build on California and make it even stronger.

Let me congratulate you, Mr. MacTaggart on accomplishing in two years a feat that Congress has been unable to do in two decades. And a extraordinary example of citizen activism and your coalition. Persevering against very strong opposition that similarly to what is happening now on a national level expressing good intentions sought to sabotage rather than advance your success.

And in fact, every week we receive a new privacy framework from trade group. They start with preemption and they conclude with endorsing the status-quo. Preempt California. Go back to the status-quo.

So, let me ask you, how would you -- what are the most important points that you think you would apply to make California even stronger at the national level?

MACTAGGART: Well, Senator I'm pretty -- I was pretty happy with

the -- with the deal we struck -- we did have to give up a couple of things. We -- we gave up a whistle blower provision. Because I do think finding out what's going on in -- inside these companies is very difficult.

And but, other than that we -- we were in this extraordinary position where the consumer companies realized they were going to have to spend a lot of money that wasn't going to look good for them spending against their customers. So, I -- I -- we -- we got a deal that we really liked.

WHITEHOUSE: And -- and -- I'm glad to hear that. And look

forward to your helping us, including members of this committee, the Judiciary Committee. Because I think the input from this committee will be important to the Commerce Committee as we frame legislation, bipartisan legislation, going forward.

Is there anyone here talking about enforcement that would be opposed to strong authority both for rule making and penalty imposition by the FTC? If you're against it, raise your hand? Is there anyone -- and the record may reflect that no one raised his hand.

Is there anyone who would oppose state Attorney General enforcement of the federal law? If you're opposed to the state Attorney General enforcement, please raise your hand. Good. No -- no one has raised your hand.

Let me ask Google are you willing to commit, Mr. DeVries, support for a law at least as strong as California, and potentially with a whistle blower provision?

DEVRIES: Senator, we support the goals of the California

legislation. There's things that can be improved. We have needs and fixes to be made as everyone acknowledged. But with those fixes I think that those are important rights that we'd want to see in federal law as well.

WHITEHOUSE: Well, I'd ask you for the record to give me in

writing what you think the fixes should be?

DEVRIES: We'd be happy to communicate those. We've been working

with the Attorney General on this issue as well as members of the legislator about what some of the changes would be to bring some of the ambiguities out of the law and make the rights more clearly stated.

We think we can even do broader -- more established those rights even more broadly as we consider a federal legislation.

WHITEHOUSE: Mr. Weinberg, one last question, because my time is

almost up. Is there a potentially a business model here? That in effect, and I think you'd proven there is. Avoids tracking but, also collects any information completely anonymously. In other words, divorcing or separating the information from name and other identifying information?

WEINBERG: Yes, Senator I do. I think the devils in the details,

as you started with. And that, when you have this notion of pseudo anonymous data, it can actually be not anonymous. But if we legislate those kind of ambiguities as required, I believe that companies will innovate and figure it out like we have.

WHITEHOUSE: If -- if we legislate that separation -- like a

separation of church and state. The companies would comply, and we would change the business model. But there would still be the opportunity for profitability?

WEINBERG: Yes, Senator, I believe that's the case.

WHITEHOUSE: And you've proven it?

WEINBERG: Yes.

WHITEHOUSE: And would that change Google's business model?

WEINBERG: As, Mr. DeVries mentioned I think Google actually

makes most of its money in a way that would not change it that significantly. They make it via contextual advertising on search ads and they've have divorce themselves from the behavioral advertising.

WHITEHOUSE: Do you agree, Mr. DeVries?

DEVRIES: I think we'd want to make sure we support publishers

with advertising products. But I -- I agree otherwise with Mr. Weinberg.

WHITEHOUSE: Thank you.

BLACKBURN: Gentleman's time has expired. And that concludes our

questioning for this first panel today. We thank each of you for being here. I think that is evident to you that we are focused on doing something.

Opting-in for your PII, making that choice, having that protection opt-out for search and non-sensitive data. Those are things that you have heard discussed here today. We look forward to continuing to talk with you all and work as we develop a privacy protection legislation. Thank you all for your time. You're dismissed.

At this time, as we reset the table for our second panel, I will call them forward and introduce them as I am calling them forward.

Ms. Roslyn Layton, is a visiting scholar at the American Enterprise Institute.

Ms. Michelle Richardson, is the Director of the Privacy and Data Project at the Center for Democracy and Technology.

Professor Jane Bambauer, and I hope I am saying your name correctly, Bambauer? Excellent. Is a Professor of Law at the University of Arizona College of Law, she is also the Director of the Program on Economics and Privacy at George Mason University Antonin Scalia Law School.

I want to welcome the three of you. I will say that it is an honor for me to see before me three women leaders in technology. This is women's history month and no doubt, you all are probably making history. This is the first time we have had a panel of women here.

Before I have you stand, and we swear you in. I'd like to ask anonymous consent to include Senator Grassley's statement for the record in the record of these proceedings. Without objection, so ordered.

If each of you will stand to be sworn in. Do you affirm that the testimony that you're about to give before this committee is the truth, the whole truth, and nothing but the truth, so help you God?

Thank you, please take your seats.

And, Ms. Layton we will begin with you with your testimony.

LAYTON: Senator Blackburn, Senator Coons and members of the

committee, thank you for the opportunity to discuss the GDPR and the CCPA. It is a honor and I'm harden by your bipartisanship. This testimony reflects my research conducted at Demark Audbur University.

Additionally, I'm the mother of three Danish American children, so I have a very personal interest to investigate whether the European rules work. The academic literature shows that online trust is a function of institutions, business practices, technology, and user knowledge.

But unfortunately, the European union rejected this formula for its data protection policy. My hope is for Congress to avoid the mistakes of the GDPR and ultimately leap-frog Europe with a better framework based upon privacy enhancing technology, consumer education, and scientifically based standard setting.

Now, to analyze a policy like the GDPR, we must set aside the political pronouncements and evaluate its real-world effects. Here are ten key problems with the GDPR and if not properly addressed they will also plague the CCPA.

The first problem. The GDPR has strengthened the largest players. Since implementation, Google, Facebook and Amazon have increased their market share in the E.U.. This is a perverse outcome for a policy promised to level the playing field.

Number two, the GDPR weakens small and medium size firms. The ad-tech competitors of Google and Facebook have lost up to one-third of their market position. And venture capital for E.U. startups has declined by one-fifth.

Number three, the GDPR is expensive to implement. Dozens of Americans firms no longer serve the E.U. because of the high cost of compliance. Some $3 million for a company of 500 employees. Given that Europe is a destination of two-thirds of America's goods and services this should be seen as a -- a tariff.

Four, the GDPR silences free speech. Over 1,000 American news sites such as the venerable Los Angeles Times and the Chicago Tribune are no longer accessible in the E.U.. If this policy was

introduced in the United States it would violate the first amendment for the barrier its creates to expression.

Number five, the GDPR threatens innovation and research. GDPR requirements are fundamentally incompatible with big data, artificial intelligence, blockchain and machine learning.

Number six, the GDPR undermines the transparency of systems that organize the Internet. The vital information of the so-called, WHOIS protocol, the address book of the Internet, is obscured today. Law enforcement, cyber-security professionals and property rights holders can no longer access this vital information.

Number seven, the GDPR and the CCPA create risks for identity theft and online fraud, because there's no requirement for -- to authenticate users before their information requests.

Number eight, the GDPR has not created greater trust online in the E.U. After a decade of increasing regulations, including lots of opt-ins, Europeans report no greater sense of trust online. California has more privacy laws than any state, and yet, its residents do not report feeling more private or safe.

Number nine, the GDPR and the CCPA use the pretense of consumer control to increase the power of government. The discussion of consumers takes just a small part of the text of these laws, whose main goal is to empower bureaucrats. The GDPR imposes 45 specific regulations on business practices and 35 obligation on regulators. There was no rational process to test these provisions before they were enacted. California goes even further with 77 invented regulations and sweeping powers granted to the Attorney General with no accountability or transparency requirements.

Number 10, because the GDPR and the CCPA fail to meaningfully incorporate the role of innovation and education in policy, they will not increase trust online. People should not be so naive to mistake the bureaucratization of data protection as a way to create a natural right of privacy.

So, I urge this Congress to attempt to create a superior framework. This will require incentivizing the development of world-class, scientifically-proven, privacy-enhancing technologies through grants and competitions and to provide safe harbors for their research, development and practice. My testimony details ways to enable consumer education.

And finally, Congress should look at the role of scientific standard setting as described by Nobel Economist Elinor Ostrom, who advocated governance where the users set the rules and offered means of monitoring and compliance that don't bankrupt the enterprise. The E.U. should not -- the U.S. should not copy the E.U. on data protection but leap-frog it by creating better systems and policies. I thank you, and I look forward to your questions.

BLACKBURN: Thank the gentle lady.

Ms. Richardson, you're recognized.

RICHARDSON: Chairwoman Blackburn, Ranking Member Coons, thank

you for the opportunity to testify today. This Center for Democracy and Technology has supported comprehensive federal privacy legislation since our founding in 1994. And we appreciate the committee taking on this issue at a uniquely important time. Privacy and data issues are often complex and full of jargon. We want to leave you with one clear message today. Our current notice and consent model is broken.

We need Congress to think much bigger instead of keeping this model limping along. Move the privacy burden back to where it belongs; the companies who collect and use our data. We've seamlessly integrated the Internet into every aspects of our lives, and it has improved the quality of our lives in extraordinary ways.

But it has also created a world where devices and applications are constantly creating and collecting data about us. We interact with smartphones, laptops, wearables, home IoT devices, connected cars, online accounts, websites and even connected public infrastructure every day.

There is little left about our lives that is not documented in some way. But the problem goes further. Our data doesn't stay with the long list of companies we consciously choose to engage with. It's instead shared with third parties and business partners that we have no relationship with. And this includes data that is incredibly sensitive like location information, biometrics and health data.

Some argue that the solution to this problem is making privacy policies clear so consumers better understand what they're signing up for. But ultimately, there is no meaningful way for people to make informed timely decisions about the hundreds of different companies that they interact with every day.

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

To that end, CDT has published model privacy legislation, and we invite members to borrow from it as they craft a comprehensive privacy bill. It's informed by GDPR and the new law in California, but we think it better reflects U.S. values and more significantly shifts the burden of data management from users to companies. It's crucial that a federal privacy law govern all entities that hold personal information and under a single regime.

We would recommend that any privacy law do four things. One, it should deter discrimination against those who use online services; two, it should limit the collection, use and sharing of sensitive information that is not necessary to offer the service the user requested; three, it should require all entities to take reasonable efforts to secure personal information; and four, it should grant individuals the right to access, correct, delete, and port their information.

Importantly, all of these requirements can and should exist outside of the current notice and consent model. These are the rights that you should not be able to sign away. We also believe these requirements should apply to businesses that process personal information regardless of the business model or their size.

And if drafted properly, these sorts of requirements can actually level the playing field. As Congress tries to find a way forward that works for both industry and individuals, it should be mindful that size is not always a proxy for privacy risk and privacy harm. And we recommend Congress consider the following things.

First, from the point of view of a consumer, the privacy harm they experience has nothing to do with how many employees a company has or how much money it makes. Cambridge Analytica had only six employees when it collected information on 50 million Facebook users. And some of the most popular apps today process the information on hundreds of millions of people before they even became profitable. Creating an exception from a privacy law for entities like this just doesn't make sense.

Second, different companies choose to use data in different ways, and their obligations will be proportional to their data use. For example, your dry cleaner or a corner store may process very minimal data while some technology start-ups process much more and can impact millions of people's privacy on day one. Privacy requirements can scale according to how a company uses data.

And third, clarity is just as important as flexibility. You'll hear that small businesses -- start-ups just need flexibility, but too much flexibility leads to uncertainty. Compliance costs should go to following the rules that Congress writes, not trying to figure out what they even are. Thank you again for the opportunity to testify. We look forward to working with the committee to draft a privacy law that works for both consumers and companies.

BLACKBURN: And we thank you for the testimony.

Professor Bambauer, you're recognized.

BAMBAUER: Chair -- Chair Blackburn, Senator Coons and members

of the committee, it's an honor to be here. And I'm delighted that you're doing the hard work of crafting a strong and sensible national privacy law. It is hard work.

I've devoted my career to understanding privacy and information law, because it's an area where detached and careful research can take you to some pretty surprising places. The best interests of consumers are not always intuitive in our digital economy. So, my goal is to share some of what I know about the possible pitfalls as you move forward.

So, first of all, as you know, time is of the essence. If the -- if the California Consumer Protection Act comes into effect, we may be in for a pretty rough ride. And we can look at what's been happening in Europe to get a sense.

So, since the GDPR took effect, there's been a significant reduction in venture capital investment all across every sector in Europe. That -- that comes with millions of dollars per week of lost investment and -- and of course, lost jobs as well, and lost services to consumers. Competition has also suffered, because firms who lose the most are the younger and smaller ones.

The CCPA is a light version of the European privacy law. And it's likely to cause a similar shock here, maybe even a greater shock, because the U.S. has been the world's hub of invention for information technologies.

So, Congress should certainly take the opportunity to stake out some -- some clear rules to protect consumers, but concrete risk and harm should continue to be the touchstone rather than consumer control.

So, I know I'm going against the grain. Why is it that I'm emphasizing harm over control? Well, at bottom, the GDPR and the CCPA create a property right -- right. So, the idea is that, as a consumer, it's your data, and you're the ultimate authority about its best uses.

The property model has so dominated national tension and debate about privacy that our live debates, basically, take it for granted. We're -- we're debating over opt-ins and opt-outs, for example, and that already assumes that privacy is a species of property, and the owner should have veto power.

To be sure consumers do want this -- do want to be in control of their information, particularly when harms are hard to define and hard to anticipate. But consumer control has its own problems and unintended side effects.

So first, it's frequently going to leave the consumer under protected for reasons that Mr. Taggart (sic) said in the first panel. Because they may opt-in or fail to opt-out. Without enough information

about the pros and cons of some kind of data arrangement.

But also, it's certainly definitely going to overprotect the consumer in many cases. Ultimately, to their detriment. When distrust or transaction costs cause new services to fail even though in fact, they would be beneficial if they were given a chance.

After all, people have always tended to be wary of new information technologies. It seems to be part of our hardwiring. And so, we should just be aware of that. Opt-in rules and other legal incentives to -- to sort of get consumers to guide -- to guard their privacy, rest on an assumption that unbalanced privacy is better for them.

But the empirical evidence does not really support this assumption. Studies that are able to actually take into account the real-world alternatives to a controversial data practice more often find that consumer benefit from the intrusive practices, even though they seem obnoxious. I've given a couple examples in my written testimony, but I want to elaborate on -- on digital advertising. Because that's come up so much in the first panel.

So, Senator Graham asked about googling information about golf, and then getting ads based on his -- his Google search results. It's true that Google, and other major companies would not lose much money from advertising revenue in services like that. But if you think about the dynamics of this process, it is the content markets that are going to really lose out.

So, we can look at what happened in the E.U. when their cookie law went into effect. Across the board, revenues were reduced for all -- all -- all websites. But the relative story's where things get interesting. General content -- content providers were the biggest losers whereas marginal niche content providers didn't have as much of an affect.

Also, noisy and moving ads tended to do better than ads that were -- that -- that were not noisy. So, we need to keep these types of unintended consequences in mind. So, if the CCPA is equivalent to a kind of tear down and rebuild of American privacy law, I recommend a significant renovation instead. And I've circulated a bill.

I know you've seen lots of bills recently. This one empowers the FTC to expand some of the work it's already done in -- in defining unfair and deceptive privacy related business practices in this area. But it also lets them build their expertise the consumers can't possibly develop to figure out what practices are going to be most harmful. Thank you.

BLACKBURN: And thank each of you for your testimony. And I

thank you for the written testimony. We realize a lot of work goes into that. And we appreciate that you take the time to do it when you agree to come before us. And you're exactly right this is an issue that we are intending to do something on this year. I'm going to recognize myself for five minutes. Four questions.

And, Ms. Richardson, I want to thank you for mentioning that we that -- that we should have one set of rules for the entire ecosystem with one regulator; the FTC.

RICHARDSON: Right.

BLACKBURN: And I -- I do think that type clarity sets the

ground rules for how we move forward.

Because Ms. Layton, as you mentioned with small business and how heavy-handed rules make it more difficult for small business. We want the Internet to flourish. And we're looking at 5G coming on. And we're looking at artificial intelligence and this spectrum of data that has been created over the past ten years.

But in that regard also, we want to make certain that people do have that expectation to privacy and do know who owns their information.

Professor Bambauer, I thank you for your continuum of work on this issue. We appreciate that. Talk -- go back into what you were just talking about and let's begin with preemption and why that is so important to exercise that.

Because you look at GDPR, and of course the E.U. would have preferred for us to go first in privacy legislation, I really think they would have liked for us to set the standard. And we should want to be setting these standards. But California with their law, talk a little bit about preemption and why we need to put that in place.

BAMBAUER: Yup. Well, I -- I don't -- I don't object to the idea

that we should be setting the standard I just do not think that California's law is setting the correct standard. It is -- it is putting the onus on...

BLACKBURN: I would agree with you on that. But talk a little

bit about why we need to exercise preemption, so we don't have 50 different laws.

BAMBAUER: Right. Yes. So, in an -- in a context where every

state potentially has a different privacy law, the compliance costs with be overwhelming. The likely result is, if a -- if a company at least has enough resources, it will comply with the most demanding standard and therefore we won't really have a laboratory of democracy. You know, we won't have -- we won't be experimenting in -- in different states because of the nature of the Internet, where services cross borders. We will have -- we will have a rush to the higher level of -- of regulation.

BLACKBURN: Ms. Layton, GDPR is on average $3 million compliance

costs for a firm in the E.U. with 500 employees. And when you're looking at that startups, that just have a couple of employees, talk a little bit about how those compliance cost. What that is going to do to smaller firms.

LAYTON: Well, I think we can see what's happened already. I

mean if you can go to Silicon Valley today and -- and startups are saying we're just not serving the E.U. And it's conceivable that they -- it's just that uncertainty is so high, that they don't even want to begin to do it.

That's a concern because Europe is a location for two-thirds of our digital goods and services. So, it's quite a large market.

BLACKBURN: Yeah. You touched on WHOIS.

LAYTON: Yes.

BLACKBURN: Which we -- which I think is important. But to

comply with a GDPR, and I can, they have a rule that allows registries and registrars to obscure WHOIS. You want to talk about that for a minute?

LAYTON: Yes. So -- so, WHOIS as a kind of address book of the

internet. And -- and it's interesting because the, you know, the WHOIS database is used by the -- everyone in the world. It's used by law enforcement and -- and property rights holders everywhere. But it isn't actually required that the information is obscured.

But -- but companies are -- are invoking the ability to obscure themselves so that when people need to find out who may be putting up a site with child pornography, for example, they can't find out who's doing it.

So, it is -- it's devastating, I think. And -- and so this is a case where it wasn't -- this was one of the consequences that the European policy makers didn't consider. And they wouldn't even listen to people who'd bring up these concerns. And so -- so here we are with the major cyber-security problem, law enforcement problem, protection of intellectual property...

BLACKBURN: Right. OK. Professor Bambauer, in the couple of

seconds I have left, let's go back to the -- the -- putting a data privacy regime in place and why should the FTC be the one to take the lead in that?

BAMBAUER: Well, they -- they have the expertise that they've

already been developing over the years to understand what types of services were downed ultimately to -- to a consumers benefit, and which ones don't.

So, it's quite important, you know, we are often focused on the practices that wind up potentially harming consumers. But another major, major role of a good regulator is to allow, you know, seemingly suspicious innovations to go forward if -- even though they seem on the surface to be creepy, if there's no real reason to suspect that they are going to cause harm.

BLACKBURN: My time's expired.

Senator Feinstein?

FEINSTEIN: Madam Chairman.

(UNKNOWN): (Inaudible) let Senator Coons go first?

FEINSTEIN: Senator Coons?

COONS: Thank you, Madam Chairman, and Ranking Member Feinstein,

I'll be brief. I have just two questions...

(UNKNOWN): Thank you, (inaudible).

COONS: ... I'd like to ask the panel. Just to continue a line

of questioning that was already under way. I agree that compliance cost has to be one of our concerns as we're trying to strike the right balance.

I'm also someone passionate about protecting intellectual property. And the Internet poses a wide range of intellectual property challenges including offers to sell counterfeit goods, widespread digital piracy. And while I support efforts to protect individual privacy, I'm concerned about reports that GDPR's make it even more difficult to identify those responsible for infringing content.

Dr. Layton, if you could just -- what safeguards do you propose for avoiding enabling illegal behavior online through increased privacy protection?

LAYTON: Well, one -- one significant example is the use of

artificial intelligence to attempt to find infringements. And under the GDPR, that itself could be illegal. So, even the ways that we would attempt to compensate for the WHOIS not being accessible, that also -- so the -- the -- the workaround would be illegal as well.

So -- so, it's just that sort of a -- of a snowballing effect that we have an original problem, and then we create a law that the cure is worse than the disease. So, it's just not wanting to go down that slippery slope.

COONS: I'll look for specific proposals. I think it is an

interesting challenge.

Ms. Richardson, you raised an excellent point that the privacy risk is not proportional to size and profitability of companies. And I'd be interested in -- in your answer and if I could Professor Bambauer's too.

What beyond increased rule making, what additional teeth and tools should we be giving the FTC in order to be more affecting in protecting data privacy? For example, when providing them with authority to oppose civil penalties for first time violations be in any way a constructive stat towards giving them more relevant authority in this space?

RICHARDSON: Absolutely. Our current system where companies get

one free bite of the apple of inappropriate behavior before they are fined is not working. And that is something that could easily be done to allow them to have original fining authority. I think they're going to need an assist from the state A.G.s. If we are talking about a system that is going to sweep in all companies who hold personal information.

It's just not going to be possible for the FTC to do that by itself. No matter how much resources we give it. But I would say also Congress just needs to give the FTC direction by putting a baseline privacy standard. Make a list of no go's, the most offensive behavior that we're seeing on the internet, so the FTC can really focus on some of the harder issues and using its rule making authority to provide detail where it is really necessary.

COON: Detail, definition. Professor Bambauer?

BAMBAUER: Yes. I -- I have to read the with (inaudible)

authority. I would hope that the FTC could define both safe harbors for -- for conduct that clearly is.

(UNKNOWN): (Inaudible).

COONS: Your microphone's not on. Thank you, Professor.

BAMBAUER: Sorry. The FTC could define safe harbors for -- to --

to find conduct that clearly is in consumer's interest. As well as I don't know what the opposite would be. Deep waters? Where, you know, conduct that clearly would violate the standard. I -- I also think that the FTC could -- could...

COONS: I think they call (inaudible).

BAMBAUER: Right. OK. Yes, that's right. They could also create

certification standards for companies to...

COONS: Right.

BAMBAUER: ... more clearly compete on privacy by signaling that

they intend to comply with -- with -- with standards that go beyond what the law would require. And civil -- I'm -- I'm not against civil penalties for first violations. I -- I -- I -- my proposal bill has -- has something for that. As long as those violations are knowing. In other words, as long as it -- it's the -- the company has a reason to understand that what they're doing violates some clear -- clear notion of privacy.

COONS: Nice quick question. Tom Lee and Will DeVries on the

previous panel talked -- did not talk directly. Both referenced portability. I only dimly grasp this, if I might Ms. Richardson, my superficial grasp of this is, there happens to be a very power social media platform, into which my family and I have invested huge amounts of photographs, and data, and memories.

If another platform came up that had stronger privacy protections that was appealing to me, I don't today have the ability, that I'm aware of, to demand of Facebook that they allow me to port to a new platform everything that I want.

So, to the question the Chair was asking previously, you know, do I really own my digital, virtual self, and how would we do that in a way that would not, as Mr. Lee raised, unintentionally then compel the new more privacy sensitive company to engage in practices in the receipt of my data that would violate their own standards. Does that make sense as a question?

RICHARDSON: Yeah. And this complicated. You're going to...

COONS: It is.

RICHARDSON: ... have to make a couple of decisions. One, just

substantively about what data you should be able to take with you but also on a technical matter how the interfaces should be working. And I think that is best kicked to NIST or another agency with that expertise.

COONS: I appreciate you raising NIST. One of my favorite

federal agencies that is completely relevant here.

Thank you very much, Madam Chair, and Senate.

BLACKBURN: It is indeed relevant, and we've worked with them

for quite a while on some of these issues.

Senator Hawley, you're recognized.

HAWLEY: Thank you very much. And thanks to the witnesses to

being here today. I -- I want to talk about property rights and particularly as it relates to data brokers. But can I just first make sure that we're all on the same page?

Do you all agree that -- that the personal information like your location, like your -- the websites you visit, like your credit card information, that that is a -- a form of property? I mean like this personal data is property. Do -- do we agree on that?

You -- you don't think so, Professor Bambauer?

BAMBAUER: No. I -- I mean, property depends on certain sets of

legal rights that rights that are -- right now, are not well defined and so it's not inevitable that -- that those will be property rights.

HAWLEY: And -- and you don't think that that should be

considered property?

BAMBAUER: No, I -- I do not. For -- no I do not. I -- I don't

think that -- so, property rights are best vested in entities and people who -- who know what is in their best interests better than any -- anyone else. They have (inaudible)...

HAWLEY: Well, that's a questions about assignment of the right.

I'm talking about the content of the right.

BAMBAUER: Right.

HAWLEY: You -- you don't...

BAMBAUER: So...

HAWLEY: ... you don't -- you're telling me, you don't think

that personal information isn't property at all?

BAMBAUER: Not only is it not, it under the first amendment

precedent that we have, it cannot. It cannot really have the same form of property protection that say intellectual property does.

HAWLEY: Well, form is different. I'm -- I'm just asking is

there a -- I'm intrigued for instance by the title of the -- of the paper that you submitted. You talk about privacy as not property.

BAMBAUER: Right.

HAWLEY: But that seems to be me to be slightly a category or

mistake. We're not talking about privacy as property, but what's property is the personal information and data. Those privacy protections for that property is a different question. I'm just trying to drill down; do you actually think that personal confidential information is -- is property? But -- and I hear you saying, that you do not think so.

BAMBAUER: I do not think so.

HAWLEY: Do -- do others agree or disagree with that?

LAYTON: I would just add to -- I would just add to that and I

would point you to the work of Pam Dixon, who would really call these -- they're shared property rights. And because the -- the way that the data's collected, it's so integrated within systems, and with other users, that it's hard to extricate.

And -- and that might be just one way to think about it. I -- I don't disagree with the importance of our Constitution and how we want to protect property from the perspective of the Constitution. But there is a technical complication here.

RICHARDSON: Looking (ph) at a high level, yes. We -- we think

in an ideal world.

HAWLEY: Well, it -- it seems to me that the -- certainly the

companies who collect these are the data brokers who collect information, they regard it as property, right? Because it's bought and sold, I mean, it's monetized. It seems strange to me to say that -- that this kind of information that is quite valuable, apparently, because I understand that there's a pretty robust market for this information .It's being bought and sold, right? I mean that seems to me it's a form of property.

And so, certainly the market's treating it as a form of property. So, then we -- we have a a fairly classic question that arises in our law in regular intervals which is how do we define that property, and then how do we -- where do we assign the rights, right?

I mean, to whom do we give the property right, and what are the rules for bargaining an exchange of that right. And this is a classic market definition question that -- that has come up repeatedly in our history and that brings me to the -- to the data brokers.

So, my understanding is, you correct me if I've got this wrong, but data brokers collect data from commercial governmental, other publicly available sources. This data can include information like bankruptcy information, voting and registrations, consumer purchase data, web browsing activities, warranty registration, and other details of consumers every day interactions. They put that together, build a user profile, and then they sell this data to other parties. Have I got that, basically right? Am I -- is -- is that correct?

So, my question is then, why shouldn't we give consumers some control? Why shouldn't they be assigned the property right in this data? That they can then, you know, we can -- we can set the default rules, right? About how that data is-- is transferred or how it can be alienated if you like to use the formal legal term. But why shouldn't we start by saying the -- we're going to to assign this data property right to consumers. Is -- is that -- is that wrongheaded? And if so, why? Or is that the right approach. Yeah, we can just go down the line. Go ahead, Ms. --

LAYTON: What -- I'll just say very quickly. I -- I certainly

respect the question, I thank you for thinking so deeply about it. What I would say is it's -- it's maybe not what's so important as the data, it may be the algorithm itself. It's the software that's the property that -- and my concern is the regulations that we are doing are in fact -- they're regulatory takings.

We are essentially taking -- divesting companies for their intellectual property to create an algorithm. The person's data is a separate issue which -- which I don't necessarily have the answer for you. But I think you need to distinguish between the data collected and the algorithm itself.

HAWLEY: Can -- can you just say more about the -- do say

something about the algorithm and why that might be proprietary and why and why it's so valuable to the companies that develop it.

LAYTON: Well, and -- and absolutely, I mean I think when we --

you -- saw the companies that we had today. It was their engineers, their ingenuity that created the -- they -- they put together the -- the rules or the -- the -- the decisions between how thing should be related. They've written that down in a code. And that code is -- has a value, which they of course want to protect, there's no doubt about that.

HAWLEY: Yeah. Thank you.

Do you have anything to add to that, Ms. Richardson?

RICHARDSON: We don't usually use up property framework to talk

about this, but we do think your number one goal should be shifting the burden of privacy management from users back onto companies.

HAWLEY: I see my time's expired.

Thank you, Madam Chair, thanks all of you.

BLACKBURN: Thank you all.

Senator Feinstein for five minutes.

FEINSTEIN: Thank you very much, Madam Chairman. Senator Hawley,

I thought your questions were very well placed and really very good. For someone, and I'm not all that computer sophisticated, it was revolutionary because I really see the breadth and depth of what we're dealing in. And the fact of what the unknown is what the future brings.

So, let me ask this the European law, I'm fascinated about this and opt-in and opt-out. It seems to me if you have a button for opt-out, you can have a button for opt-in. But how -- how -- how would you respond to claims that the European law has been harmful for business? Please.

RICHARDSON: I -- I would point out that it's only been nine

months and there is not a lot of good data out there about how this is really affecting businesses. Either there, or here in the U.S. There are some statistics available, but they are really looking at very small snapshots of very specific things.

But there is some hope. I know Cisco recently put out a report that said that companies that are GDPR compliant are getting their products out faster. Because there are fewer questions about privacy and security. So, we're hoping that we're moving to a model where people benefit from the investment up front.

LAYTON: Senator, as a person who lives in the E.U., and

experienced that for the past decade, with increasing waits of privacy regulation, I would say it is -- it's quite demonstrably worse. Particularly as an American. If you want to read American news. You cannot access over 1,000 news sites from the European Union. You can't read what's going on in the Los Angeles Times. You just a get blank -- a -- a white page that says due to the GDPR, we're not serving content.

So, that -- it's -- it's staggering to think about what, you know, from American perspective what that would mean, if -- if we would adopt such a framework. But from the other side, the -- the opt-in kind of the way that it's experienced, every single time you go to a new website this big popup comes into your face.

And what's -- what has been shown in consistent user studies is people frequently click away. Or they do the opt-in and then they have to -- they don't read the policy, so much more data's collected had they not had an opt-in.

And this has also been shown with do not track, is that companies who will say opt-in up front, they tend to ask for more points to collect on data than had they not. So this is one of the unintended consequences. I know it sounds great on the surface, but in practice, can have a negative effect.

BAMBAUER: So, it's true that the...

FEINSTEIN: (Inaudible).

BAMBAUER: ... the GDPR has -- has obviously only been in effect

for a few months and that -- that the studies -- there are some, you know, well done studies but they are limited by -- by that fact. Europe was already starting though from a very strong privacy standpoint. And so, the fact that we're seeing so much -- so much of an effect, suggests that here in the U.S., when we move form a lower baseline to a -- to a much higher one that -- that -- that the impact may be greater.

But let me tell you about another study here in the U.S., actually, in your district. There was a study of opt-in versus opt-out for -- for lending. Because it just happened to be that counties in the bay area took different default approaches.

So, in one county, you know, they would require -- if a -- if a bank wanted to get extra data from these data aggregators, the -- the person applying for the loan would have to opt-in and in another county, similar county, they'd have to opt-out if they didn't want that data collected.

So, the result was that the counties with opt-out procedures, where for most applicants, data was automatically, you -- you know, was automatically received from data aggregators. Those applicants got better loans. The terms were better, the -- the interest rates were lower on average, and the defaults were -- were...

FEINSTEIN: Why would that be?

BAMBAUER: Why would it be? It's because loan officers are

always going to work with some information. They will definitely have income. If you also think about the distributional affects, this is important too, loan officers are always going to be making their decisions based on income.

So, we already have a class, you know, a sort of class effect. With extra information though, you can differentiate the people who may look bad by traditional members -- by -- by traditional measures, but who are actually low credit risk based on this extra sort of new information that was collected about them passively.

And -- and therefore, offer loans to -- to otherwise weak looking applicants who are not actually likely to default. And then, you know, conversely, if we're limited to just the basic information that an applicant providers, because they have, you know, failed to opt-in to extra sort of creepy sounding data practices, well, ironically, they're actually going to be disserved by that.

FEINSTEIN: But as I understand it, we're talking about all

kinds of data now, the most personal data and the most impersonal data. It seems to me, that on opt-out, the individual loses their power.

BAMBAUER: Yes.

FEINSTEIN: But in opt-in, the individual has the power to say

no, I don't want you to collect this or do that. And what I worry about, because of the sophisticated of the sector, is that it becomes so complicated, that people rebel against it. And I know when I get some of these notices, I don't know what they mean, the print is so small. The easiest way is just to avoid it.

But if I have to get something, I'm going to find a way to get it and that to me is kind of the different between opt-in and opt-out and maybe you limit the areas but I -- I think everybody would agree that an individual's personal medical data should have the highest security connected to it. And that you would want to opt-in to anything that offered the opportunity that you lose some of that security, and say no.

So, I have a very, as somebody who is sort of a -- of a generation that is not the most hip in terms of these things, I want to see that people are protected. And our privacy is protected. And I know I'm a Californian, I know the industry somewhat, and appreciate it and want to help it. But the power they have is so enormous over individuals that they know all this, and the individual knows a very little bit about how something may be used and -- you're -- you're going to, you know, face exposure that's going to identify you and that kind of thing.

When you think of what the future can bring, I would think that the United States of America in terms of the federal government, would want to protect people as much as they possibly could. I'd be interested in your comments.

BAMBAUER: So, is it OK to go over...

BLACKBURN: Time has expired. And I will -- if it is OK for us

to take their comments as a written response.

FEINSTEIN: Fine.

BLACKBURN: That would be appreciated. I -- there are no other

members waiting to ask questions, and we want to thank you all for your time being here today for your testimony. I will remind all the members of the committee that you have one week in which to submit additional questions for response. While on the Senate side, they do not put a time limit on you, for like we did when I was in the house.

Let's just do that in a very timely manner. As you can see, this is an issue that's we want to take an action on. To make certain that we find that right balance. That your PII is protected, that your non sensitive information has protections, but it properly utilized, that we exercise the data security which deals with the breaches, and the notifications there and that as we look at intellectual property protections, that we also look at prioritization.

And what is being done in the search field on prioritization. With that, we thank you all for being here.

This hearing is concluded. Adjourned.

END

Mar 14, 2019 11:08 ET .EOF

-0- Mar/14/2019 15:08 GMT