S. HRG. 115–895

CONSUMER DATA PRIVACY: EXAMINING LESSONS FROM THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION AND THE CALIFORNIA CONSUMER PRIVACY ACT

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

OCTOBER 10, 2018

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

58–559 PDF WASHINGTON : 2025

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER WICKER, Mississippi	BILL NELSON, Florida, *Ranking*
ROY BLUNT, Missouri	MARIA CANTWELL, Washington
TED CRUZ, Texas	AMY KLOBUCHAR, Minnesota
DEB FISCHER, Nebraska	RICHARD BLUMENTHAL, Connecticut
JERRY MORAN, Kansas	BRIAN SCHATZ, Hawaii
DAN SULLIVAN, Alaska	EDWARD MARKEY, Massachusetts
DEAN HELLER, Nevada	TOM UDALL, New Mexico
JAMES INHOFE, Oklahoma	GARY PETERS, Michigan
MIKE LEE, Utah	TAMMY BALDWIN, Wisconsin
RON JOHNSON, Wisconsin	TAMMY DUCKWORTH, Illinois
SHELLEY MOORE CAPITO, West Virginia	MAGGIE HASSAN, New Hampshire
CORY GARDNER, Colorado	CATHERINE CORTEZ MASTO, Nevada
TODD YOUNG, Indiana	JON TESTER, Montana

NICK ROSSI, *Staff Director*
ADRIAN ARNAKIS, *Deputy Staff Director*
JASON VAN BEEK, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

CONTENTS

WITNESSES

APPENDIX

CONSUMER DATA PRIVACY: EXAMINING LESSONS FROM THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION AND THE CALIFORNIA CONSUMER PRIVACY ACT

WEDNESDAY, OCTOBER 10, 2018

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m. in room SR–253, Russell Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Wicker, Blunt, Fischer, Moran, Capito, Gardner, Young, Nelson, Cantwell, Klobuchar, Blumenthal, Schatz, Markey, Udall, Duckworth, Hassan, Cortez Masto, and Tester.

OPENING STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Good morning.

Today we are holding our second hearing on needed safeguards for consumer data privacy. As we consider potential Federal legislation on privacy, it is essential that we hear from stakeholders and experts with varying perspectives to inform our work.

Two weeks ago, we heard from major technology companies and Internet service providers about how they are seeking to address consumer privacy, and their efforts to comply with the European Union's General Data Protection Regulation, or GDPR, and the new California Consumer Privacy Act, or CCPA.

While the experience of such companies is important to consider, I want to be clear that the next Federal privacy law will not be written by industry. Any Federal privacy law should incorporate views from affected industry stakeholders and consumer advocates in an effort to promote privacy without stifling innovation.

With that in mind, today's hearing will focus on the perspectives of privacy advocates and other experts. We will also continue to solicit input from additional stakeholders in the days ahead.

GDPR and CCPA have undoubtedly spurred our conversation about a national privacy framework, and they give us useful examples as we contemplate Federal legislation. Of course, congressional action on privacy is not entirely new. Over the last several decades, Congress has enacted legislation to protect children, healthcare, and financial information.

Privacy debates have been ongoing in multiple sectors. Even the recently enacted FAA Reauthorization includes provisions on privacy specifically regarding the use of unmanned aircraft systems for commercial purposes.

Federal agencies, such as the Federal Trade Commission and the Department of Commerce, have also performed longstanding roles regarding privacy and have been increasingly active recently in this area.

At the same time, I am well aware that Congress has tried, and failed, over the last few decades to enact comprehensive privacy legislation. To be successful this time, we all must endeavor to keep open minds about the contours of a bipartisan bill.

In the wake of Facebook's Cambridge Analytica scandal and other similar incidents, including a vulnerability in Google Plus accounts reported just this past week, it is increasingly clear that industry self-regulation in this area is not sufficient. A national standard for privacy rules of the road is needed to protect consumers.

At the same time, we need to get this right. Passing onerous requirements that do not materially advance privacy would be a step backward. While it may be too early to determine the impact that GDPR and CCPA will have in the U.S., the most notable difference most consumers can see directly has been the increase in GDPR-inspired pop-up notices and cookie consent banners on their devices.

As we continue to work toward a possible legislation, I encourage my colleagues to challenge what industry told us at our first hearing, but also to examine both the potential benefits as well as the potential unintended consequences of the new rules put forth by the European Union and the State of California.

I want to say thank you to our panelists for being here today, and we will look forward to hearing from you in a just a minute.

I will turn to our Ranking Member, the Senator from Florida, Senator Nelson, if you would like to make an opening statement.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Mr. Chairman, again, under your leadership in this committee, I will be retuning to the panhandle of Florida.

I want to say kudos to you because the assets that we have authorized in this committee, an overhead for NOAA, as well as the second airplane that flies at 40 to 45,000 feet which has dramatically improved the National Hurricane Center's ability to project the path and the ferocity of a hurricane.

In two hours this is hitting landfall at ground zero about Panama City. That track has been solid there. So the local authorities have had ample warning and the National Hurricane Center was right on the money. A lot of that ability to forecast so accurately has come because this committee has authorized the assets.

I just want to say that this is a big one. When you get above 100 miles an hour, the destructive force goes up exponentially. Because of the hot water of the Gulf, it has fueled it up to 140 miles an hour with wind gusts up to 170. That will just about level most any structure unless it is made of concrete and steel.

That is the destructive force that we see approaching the Florida coast right now, and I will be going back to Florida as soon as we pass the water bill.

All of the agencies that this Committee has jurisdiction over, such as the Department of Transportation, the Coast Guard, and the NOAA, I visited with those representatives in the Emergency Operations Center in Florida just the other day.

So I just wanted to make that statement before I am taking off.

[The prepared statement of Senator Nelson follows:]

PREPARED STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Thank you, Mr. Chairman. As you're aware, at this very moment Hurricane Michael is bee-lining toward the Florida Panhandle and already making its presence felt. As you can imagine, my thoughts and focus are getting folks the assistance they need once the storm has passed and it's safe for residents to assess the damage.

Hurricanes are part of life for a few of us who serve on this committee. And, as we all know, disasters are events that bring people together to help each other out.

A number of personnel from agencies under this committee's jurisdiction—such as the Coast Guard, NOAA and the Department of Transportation, among others, have already been hard at work preparing for the storm. And, they are prepositioned and ready to assist in Michael's aftermath. I'm grateful for these hardworking and dedicated public servants and stand ready to roll up my sleeves and work beside them to help my fellow Floridians in the coming days and weeks.

With that, Mr. Chairman, I'm going to excuse myself from today's proceedings so I can give my full attention to monitoring the situation on the ground in Florida.

The CHAIRMAN. Thank you, Senator Nelson. Be assured that you and your constituents, and our first responders, will be in our prayers. Godspeed and be safe as you travel down there.

Thank you.

Senator Markey, I think, has an opening statement.

STATEMENT OF HON. EDWARD MARKEY, U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman. Thank you for having this very important hearing.

Again, all of our thoughts and prayers are with the Gulf Coast and this incredible storm, which is about to hit Senator Nelson and all the people of Florida, and any of the adjoining states that might be hit by this storm as well.

I appreciate this opportunity to discuss a priority that I have personally worked on for years, which is protecting Americans' privacy. Data is the oil of the 21st century. It fuels all of the services—the applications, the websites—that improve our quality of life and make America competitive in today's digital world.

While the data-driven economy has undoubtedly revolutionized the way we communicate and conduct commerce, too often these changes have come with an unexpected cost to users. Many data-driven services use their customers' personal information as a commodity, collecting, using, sharing, and selling individuals' personal information without users' knowledge or permission.

Consumers are frequently unaware of these practices, and have no reasonable means to stop companies from mining and using their personal data for unwanted, intrusive purposes.

Last month, this committee listened to the perspective of a few major industry players, and I was pleased to hear Apple, Google,

Twitter, Amazon, Charter, and AT&T finally agree that Congress must enact a comprehensive Federal privacy law. But we should not have any delusions about why those companies and their peers are all of a sudden advocating for a Federal privacy law.

It is clear that they are coming to the table because they now have to comply with a European privacy law and even more motivating, they will soon have to comply with a California privacy law. Their hope is that Congress will pass a comprehensive Federal privacy bill that preempts California and perhaps other more burdensome future State laws.

But before we even begin to have a conversation about preemption, we need to agree on a strong set of standards that give Americans true privacy protections.

Today's hearing is critical because we have the opportunity to hear from experts in consumer privacy about what that strong set of standards should look like.

Our goal throughout the process must be to give Americans meaningful control over their personal information, while maintaining a thriving, competitive data ecosystem in which innovators and entrepreneurs can continue to develop and flourish. That is what we are here today to discuss.

I am supportive of strong Federal privacy legislation. That bill should begin with the principle of knowledge, notice, and no. Consumers need knowledge that their data is being used or shared, notice when their data is compromised, and the ability to say no to entities that want their personal information. These are the principles of my CONSENT Act, which I have introduced.

But these are nothing more than just merely the starting points on this discussion because notice and choice are simply not enough. Transparency and opt-in consent are just the beginning. American privacy laws should also include limits on how companies can use consumers' information.

The bill should prohibit companies from giving financial incentives to users in exchange for their personal information. Privacy must not become a luxury good that only the fortunate can afford.

The bill should ban take it or leave it offerings in which a company requires a consumer to forfeit their privacy in order to use a product. Companies should not be able to coerce Americans into providing their personal information by threatening to deprive them of a service.

This privacy bill of rights should include the rights to access, correct, and delete your personal information that is held by a private company.

The legislation should stop companies from collecting vast troves of users' personal information that have nothing to do with the company's offerings. They should only collect that which is absolutely necessary to carry out the service.

The bill should require companies to keep their customers' private information safe and secure. And we must make that daily data breaches a thing of the past.

The legislation should include special protections for children and teens who have a right to grow up and make mistakes without being monitored at every turn. Most notably, we need to extend

special protections to 13, 14, and 15 year olds who today enjoy no protections whatsoever.

Finally, we must give the Federal Government and states strong enforcement powers. The Federal agency in charge of executing the law, whether it is the Federal Trade Commission or another existing agency or a new entity, must have robust rulemaking authority in order to ensure the rules keep pace with changing technologies.

I am confident that we can write that bill in a bipartisan way. We can give Americans their long overdue privacy bill of rights and still allow our economy to thrive.

I am willing, and I think all members are willing, to work together to write this bill in a bipartisan way.

I am looking forward to receiving the guidance from the witnesses today. I thank you all for being here.

I yield back to you, Mr. Chairman.

The CHAIRMAN. Thanks, Senator Markey.

We are very pleased to have with us today a great panel. Dr. Andrea Jelinek, who is the Chair of the European Data Protection Board; Mr. Alastair Mactaggart, who is the Board Chair of Californians for Consumer Privacy; Ms. Laura Moy, who is the Executive Director and Adjunct Professor of Law at Georgetown Law Center on Privacy and Technology; and Ms. Nuala O'Connor, who is President and CEO of the Center for Democracy & Technology.

Thank you all for being here. We look forward to hearing from you. We would ask you, if you can, to confine your oral remarks to as close to 5 minutes as possible. Your entire statements will be made a part of the permanent record.

Welcome and we will start on my left, and your right, with Dr. Jelinek. Welcome. Please proceed.

STATEMENT OF DR. ANDREA JELINEK, CHAIR, EUROPEAN DATA PROTECTION BOARD

Dr. JELINEK. Thank you.

Chairman Thune, Ranking Member Markey, and distinguished members of the Committee.

My name is Andrea Jelinek. I am the Head of the Austrian Data Protection Authority and the Chair of the European Data Protection Board.

Thank you for inviting me to address you on the European Union's General Data Protection Regulation or GDPR. As Chair of the European Data Protection Board, which brings together the national supervisory authorities and the supervisor in charge of the European institutions, my task is to make sure we are all on the same page because a key task of the Board is to ensure the consistent application of the GDPR and to provide guidance to this end.

My aim today is to shed some light on how the GDPR works and the concepts behind it. I hope this testimony contributes to the extremely timely debate on the possible adoption of a comparable law in the U.S. at the Federal level.

The volume of digital information in the world doubles every 2 years, artificial intelligence systems and data processing deeply modify our way of life and the governance of our societies. If we do not modify the rules of the data processing game with legislative

initiatives, it will turn into a losing game for the economy, society, and for each individual.

Both in the U.S. and in the E.U., people are more vocal about their rights to data protection than ever before. The Facebook data breaches, or misuse of data and other revelations, have caught peoples' attention, up to a point where it is necessary to reestablish trust. Trust has always been at the core of the economy and this is even truer in today's digital society.

More legislators and business leaders are stepping forward to say the time for overarching, Federal level privacy legislation in the U.S. has come. I think, for example, of Brendan Eich, CEO of Brave Software and former CEO of Mozilla, who wrote to this very committee making the case for GDPR-like standards. What shape should such a law be? And this is, of course, up to the U.S. policymakers to decide. The E.U.'s GDPR and its functioning can serve, maybe, as an inspiration.

Is the GDPR the perfect recipe? Actually, it is the result of an intensive consultation and collaboration process with all stakeholders and builds on rules that have been in place in Europe for more than 20 years.

Under the GDPR, data can only be processed on the basis of core principles, including the requirement that data collection and processing shall be lawful, adequate, accurate, transparent, proportionate to the purpose for which it is undertaken, and kept only for as long as necessary. Individuals must be informed about the main aspects of the processing of their data, and are empowered to exercise rights on their data, such as to obtain access or demand erasure when the data is incorrect or processed unlawfully.

Accountability is one of the GDPR's core principles and the E.U. was inspired in this aspect by some of the principles stemming from your common law system. It relies heavily on a businesses' capacity to self-regulate.

Organizations are responsible for complying with the GDPR and must be able to demonstrate their compliance.

The market offer of new privacy or data security enhancing products is growing. In other words, investing in privacy pays off and creates new commercial opportunities. Data protection is a unique selling proposition.

One of the greatest achievements of the GDPR is the one stop shop mechanism, which means a single lead supervisory authority is responsible for drafting a decision in a cross border compliant case or a data breach case. International or multinational companies operating in different countries have only one interlocutor to deal with: the Lead Supervisory Authority is in the country in which the company has its main E.U. establishment. Any decisions taken by the lead supervisory authority are valid across the European Union.

As European data protection authorities, we have rolled up our sleeves and actively engaged in a dialogue with stakeholders. This has included the adoption of 18 sets of detailed guidelines on many aspects of the GDPR, following broad public consultations to which many U.S. companies contributed. This work will continue, as new questions will keep emerging.

How do we ensure that the GDPR is enforced? The 2 percent or 4 percent numbers that are often reported are maximum ceilings that will only apply to the most serious infringements. Fines are a last resort, just one of the tools which data protection authorities can use to enforce the GDPR and only after a thorough investigation of the facts and always on the basis of the specific circumstances of each case. Fines must be effective, proportionate, and dissuasive.

As European data protection authorities, we stand ready to share our experience and expertise, and further discuss these issues with all interested parties.

Let me conclude with the words of one of the greatest U.S. legal experts, and one of the founders of modern privacy law, Louis Brandeis, "The right to be left alone [is] the most comprehensive of rights, and the right most valued by free people." Ninety years have passed since Justice Brandeis so eloquently captured what privacy is about, but these words have never been truer than they are today in our digital world.

Thanks for your attention, and I will be happy to answer your questions.

[The prepared statement of Dr. Jelinek follows:]

PREPARED STATEMENT OF DR. ANDREA JELINEK, CHAIR, EUROPEAN DATA PROTECTION BOARD

Mr Chairman, Honorable Senators,

My name is Andrea Jelinek, I am the Head of the Austrian DPA and the Chair of the EDPB.

Thank you for inviting me to address you on a piece of legislation that has caused quite a few ripples in Europe and beyond, the European Union's General Data Protection Regulation or GDPR.

As Chair of the European Data Protection Board, which brings together the national supervisory authorities and the supervisor in charge of the European institutions, my task is to make sure we are all on the same page. A key task of the Board is to ensure the consistent application of the GDPR and to provide guidance to this end. My aim today is to shed some light on how the GDPR works, and the philosophy and concepts behind it. I hope this testimony contributes to the extremely timely debate on the adoption of a comparable law in the US, at Federal level.

It is often asserted that the EU and the U.S. have a different approach to privacy and freedom of information, based on different historic backgrounds. In the EU, secrecy of communications and the protection of personal data are enshrined in the European Charter of Fundamental Rights. Europe's complex history has shaped its views on privacy and data protection and caused EU citizens to be in favour of strict data protection rules. Does that mean Americans are less worried about the protection of their personal data than Europeans are? It doesn't seem that way.

24 percent of social media users in the U.S. are not at all confident in the ability of these platforms to keep their personal information safe.*

And 64 percent of Americans have experienced a significant data breach pertaining to their personal data or accounts. We can only expect that number to go up with the latest Facebook revelations.*

The volume of digital information in the world doubles every two years, artificial intelligence systems and data processing deeply modify our way of life and the governance of our societies. If we do not modify the rules of the data processing game with legislative initiatives, it will turn into a losing game for the economy, society and for each individual.

Both in the EU and the U.S. people are more vocal about their right to data protection than ever before. The Facebook data breaches or misuse of data and other revelations have caught people's attention, up to a point where it is necessary to re-establish trust. Trust has always been at the core of the economy and this is even more true in today's digital society.

---

* Pew Research Centre

Businesses have started coming around too. And not just because they need to comply with the GDPR, but because they see that their clients and employees alike expect their personal data to be treated in a safe manner.

More legislators and business leaders are stepping forward to say the time for overarching, Federal level privacy legislation in the U.S. has come. I think, for example, of Brendan Eich, CEO of Brave Software and former CEO of Mozilla, who wrote to this very committee making the case for "GDPR-like standards". What shape such a law should take is of course up to U.S. policy makers to decide. The EU's GDPR and its functioning can perhaps serve as an inspiration.

Is the GDPR the perfect recipe? Maybe not, but it is the result of an intensive consultation and collaboration process with all stakeholders and builds on rules that have been in place in Europe for more than 20 years. The GDPR does not change these rules but ensures greater effectiveness. We often describe this as an evolution rather than a revolution.

The GDPR is designed to ensure, as a single set of rules, the data protection rights and liberties of data subjects in the EU. The harmonisation of the legal landscape means two things: one overarching law rather than sectoral rules and the principle of "one continent, one law". These "common rules of the game" create a level playing field and ensure that data can move easily between operators, while guaranteeing the consistent protection of individuals. The goal is to have one set of privacy rules that are interpreted in a uniform way throughout the continent. This represents a significant reduction in compliance costs for companies active in more than one EU country, as well as increased legal certainty. These are very tangible benefits of the GDPR, especially for foreign operators and smaller companies that do not always have the resources to deal with complex and diversified legal environments.

Under the GDPR, data can only be processed on the basis of "core principles", including the requirement that data collection and processing shall be lawful, adequate, accurate, transparent, proportionate to the purpose for which it is undertaken and kept only for as long as necessary. Individuals must be informed about the main aspects of the processing of their data, and are empowered to exercise rights on their data, such as to obtain access or demand erasure when the data is incorrect or processed unlawfully.

The philosophy behind the GDPR is to put individuals at the centre of privacy practices, building on human rights and values like dignity. Companies must take a closer look at what data they are collecting, what they use it for, and how they keep and share it.

Accountability is one of the GDPR's core principles and the EU was inspired in this aspect by some of the principles stemming from your common law system. It relies heavily on businesses' capacity to self-regulate. Organisations are responsible for complying with the GDPR and must be able to demonstrate their compliance.

The so-called "risk-based approach" which you find at the heart of the GDPR means that operators that limit the impact of their processing operations are exempt from a number of obligations. This approach reduces the regulatory burden for companies that carry out basic, mundane processing operations. It also creates incentives to develop innovative, privacy-friendly solutions from the earliest stages of development—"privacy by design". The market offer of new privacy or data security enhancing products is growing. In other words, investing in privacy pays off and creates new commercial opportunities.

One of the greatest achievements of the GDPR is the 'one-stop-shop' mechanism, which means a single lead supervisory authority is responsible for drafting a decision in a cross-border case. International or multinational companies operating in different countries have only one interlocutor to deal with: the Lead SA is in the country in which the company has its main EU establishment. Any decisions taken by the lead supervisory authority are valid across the EU.

How does this work in practice? When a cross-border complaint is filed, the cooperation mechanism kicks in. The LSA acts as the main point of contact and drafts a preliminary decision. This decision is then shared with the SAs concerned.

If no objections are raised, the SAs are deemed in agreement with the draft decision.

If objections are raised and the LSA decides to reject them, the so-called consistency mechanism is triggered and the case is referred to the European Data Protection Board. The Board will then act as arbitrator and issue a binding decision. On the basis of this decision, the LSA will adopt its decision (which can be challenged by the courts). The "one-stop-shop" mechanism significantly reduces the administrative burden for organisations as they do not need to consult with different regulators but receive one single position applicable in all EU countries. Complainants too only have one point of contact, *i.e.,* the supervisory authority in their country.

It is often said that the U.S. approach to data protection promotes technological innovation and economic growth, which is important for people living on both sides of the Atlantic. Let me give you my opinion on that: without trust, there is no economic growth and no innovation at the end of the day. That being said, the GDPR is carefully calibrated so as to not hinder economic development, while keeping in mind the fundamental right of the individuals.

One of the main goals of the GDPR was actually to enable a more functional information economy within the EU with more transparency for citizens, which should lead to more trust. Companies should be allowed to continue to use and share data, as long as they do so in a transparent and lawful manner, respecting the rights of individuals. The key lies in establishing an equilibrium between the respect of personal data and the commercial use of data collection and management. That equilibrium had become impossible to maintain without a new legislative initiative supported by all stakeholders.

It has only been four months since the entry into application of the GDPR, but the first responses from the business community are largely positive. Businesses have made substantial efforts to be compliant and to restore trust with consumers. There are countless examples of businesses asking their customers with straightforward and clear sign-up forms whether they can process customers' personal details with easy-to-understand explanations as to why the company needs these data.

As European data protection authorities, we have "rolled up our sleeves" and actively engaged in a dialogue with stakeholders. This has included the adoption of 18 sets of detailed guidelines on all novel aspects of the GDPR, following broad public consultations to which many U.S. companies contributed. This work will continue, as new questions will keep emerging.

How do we ensure that the GDPR is enforced? The European supervisory authorities are not the fining machines we've been made out to be by some. The 2 percent or 4 percent numbers that are often reported are maximum ceilings that will only apply to the most serious infringements. Fines are a last resort, just one of the tools which data protection authorities can use to enforce the GDPR and only after a thorough investigation of the facts and always on the basis of the specific circumstances of each case. Fines must be effective, proportionate and dissuasive.

Supervisory Authority corrective powers also include: the issuing of warnings and reprimands, ordering a company to bring processing operations in compliance with the GDPR within a specific time frame; ordering the controller to communicate a data breach to the public and imposing a ban on processing.

I hope and trust that my testimony on the GDPR and its first effects might contribute to your debate on the need for a U.S. data protection law at Federal level. I'm grateful to be here with you today and thank you again for the invitation to share our views. As European data protection authorities we stand ready to share our experience and further discuss these issues with all interested parties.

Let me conclude with the words of one of the greatest U.S. legal experts and one of the founders of modern privacy law, Luis Brandeis: the "right to be left alone [is] the most comprehensive of rights, and the right most valued by free people". Ninety years have passed since Justice Brandeis so eloquently captured what privacy is about but these words have never been truer than they are today in our digital world.

The CHAIRMAN. Thank you, Dr. Jelinek.

Mr. Mactaggart.

STATEMENT OF ALASTAIR MACTAGGART, CHAIR, CALIFORNIANS FOR CONSUMER PRIVACY

Mr. MACTAGGART. Chairman Thune, Ranking Member Markey, and members of the Committee.

Thank you for this opportunity to testify today. It is an honor and a privilege.

I come to you as the Chairman of Californians for Consumer Privacy, a group that sponsored a ballot measure which resulted in the passage last June of the California Consumer Privacy Act, or CCPA.

I also come to you as a father of three little children, concerned about the world they are growing up in. A world in which potentially every step and test they take and every decision they make

will be tracked and sold to thousands of companies they have never heard of.

Finally, I come to you as a businessperson. I am going to touch on this because this is, after all, the Senate Commerce Committee, and you heard from representatives of giant corporations only 2 weeks ago that the sky will essentially fall if you leave CCPA intact. This law was rushed and badly drafted, they said, and it needs preemption right away.

Well, I just want to say in public that I feel I am someone who, I am sure like all of you, feels that commerce is one of the most potent forces for good in this country. I make my living in northern California where many of these tech giants are headquartered. Let me assure you that I have no wish to hurt either our state's or our country's economy.

Neither I, nor CCPA, are anti-business. The law was not rushed. On the contrary, we spent years talking to legal and technical experts, academics, businesses, and privacy advocates, and its language reflects thousands of hours of careful drafting.

Now, before I describe CCPA's three main elements, it is important just to remember that it only covers large businesses with over $25 million in annual revenue, and data brokers buying and selling personal information.

The first component of CCPA is the right to know, which will allow Californians the right to find out what information corporations have collected about them.

Next is the right to say no, which allows Californians to tell businesses to stop selling their personal information. Now, our rationale is simple, you are already paying these corporations either with your wallet or your eyeballs. But their business proposition is totally one sided, either have a cell phone, use the Internet, and watch your information get sold, or go live in the Stone Age. We think that is not right.

CCPA has a sensible solution; it allows companies to collect and use your information, including importantly, to advertise to you. It just does not give them a license to resell that information for the rest of your life if you do not agree.

The final major piece of CCPA involves data security. CCPA requires corporations to take basic measures to keep California's data safe. The world has changed post-Cambridge Analytica, which members of this committee know better than anyone, and data security is near and dear to voters' hearts. Companies need to do a better job taking care of our information.

I entered this effort because I learned of a world where corporations are using your digital footprint to track you across the majority of the world's websites whether you know it or not, creating a detailed profile of you and using it to take advantage of your life circumstances, whether they think you might be considering divorce, pre-diabetic, or a persuadable and gullible voter.

Every click of your mouse and every term you search for helps create a digital file on you that dwarfs what any intelligence agency has ever known about its citizens.

We understand that this committee is considering a national standard for data privacy, but we implore you not to weaken or undo the safeguards CCPA has so recently put in place, which now

cover 40 million Americans. One in eight Americans is now covered by this law.

A law, I might add, that consistently pulled at 80 percent and above. A law which 629,000 voters petitioned to put on the ballot, and a law which passed out of both Houses of our State legislature unanimously. That is right; not a single democrat or republican voted against this law and that is because privacy is not a partisan issue. All voters care deeply about it.

Thank you for your time. We are committed to making sure that any national privacy legislation allows Americans the choice to take meaningful control over their information and their children's information.

[The prepared statement of Mr. Mactaggart follows:]

PREPARED STATEMENT OF ALASTAIR MACTAGGART, CHAIR, CALIFORNIANS FOR CONSUMER PRIVACY

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee: Thank you for the opportunity to testify about the background, rationale and intent of the California Consumer Privacy Act ("CCPA") of 2018, passed on June 28, 2018.

CCPA Principles:

Transparency

Our initial conviction was that for consumers to properly control their own data, they first need to understand what information is being collected about them. The right to find out what data a company has collected about you is the first step in understanding the scope of the issue—once you know what companies have collected about you, you can decide whether their data collection and sharing practices present a problem. Our approach was guided by Justice Brandeis' famous quote, in that making clear what is now completely opaque, seemed worthwhile: any unsavory practices would not survive the cleansing light of day.

Control

It seemed to us that knowledge would inevitably lead to a desire on the part of consumers, to be able to control the information they uncovered. This conviction led to the "Right to Say No," the right for a consumer to tell a corporation not to sell or share his or her personal information. It's one thing to do business with a company intentionally, but we heard from many advocates and consumers that the most objectionable part of this new, data-driven economy, was that their daily interactions ended up in the hands of hundreds of corporations they'd never heard of.

The right to control who could obtain your personal information, seemed fundamental to any law designed to increase consumer privacy.

Accountability

The final component of our approach, was the piece designed to address data security. Of all the areas we surveyed around personal information, the one that most concerned Californians (and frankly enraged them), was the repeated instances of companies collecting their sensitive information, and not protecting it adequately from theft. Data breaches have become daily news events, and Californians—and, we venture to guess, all Americans—are tired of giant corporations being careless with their sensitive personal information.

CCPA Background:

In settling on our approach, we met with dozens of legal and technical experts around the country, with businesses and privacy advocates. Essentially the 18 months starting January 2016 was spent on research, which allowed us to settle upon the three pillars outlined above of Transparency, Control and Accountability.

Once we had settled on this architecture, we began drafting the actual bill in the summer of 2017, and submitted a version to the California Attorney General in September 2017.

The California initiative process includes an opportunity for any interested party to meet with the Legislative Analyst's Office to give feedback on a proposed initiative, and many groups from businesses to privacy advocates took advantage of this opportunity to give comments to the LAO.

Subsequently, we met with the LAO to review this response, and were so impressed by their suggestions that in mid-October 2017 we refiled a second version of the initiative, because we felt that would allow us to improve certain aspects of the law.

That second version received its Title & Summary from the Attorney General's office in mid-December, 2017.

From Initiative to Legislation

Once we received the Title & Summary, we began the necessary steps to enable us to put the measure on the 2018 ballot. From January to May of this year, we obtained the signatures of 629,000 Californians in support of our measure. This was greatly in excess of the legal minimum of 366,000 signatures, and the measure qualified for the November ballot.

California has a relatively new provision in the initiative statute, which allows a proponent to withdraw a measure which has qualified for the ballot. We had been in contact with members of the California Legislature, notably Senator Robert Hertzberg and Assemblymember Ed Chau, and in June of 2018 reached a compromise with those two members on language that we felt would achieve substantially all of our initiative's goals. Assembly Bill 375 was subsequently voted out of both houses unanimously, and signed into law by Governor Brown, on June 28, 2018. (I should note that without the herculean efforts of Mr. Chau and Mr. Hertzberg, or the support of both Assembly Speaker Anthony Rendon's and Senate Pro Tem Toni Atkins' offices, the bill would never have become law, and much credit must go to that group of legislators for recognizing the importance of this issue, and the opportunity for California to become a leader in this field.) Additionally, Common Sense Media supported and co-sponsored the bill.

Differences between the Initiative and the Law

The 'deal' that allowed the initiative to become law revolved around three main components:

(1) *Increased consumer rights:*

a. Right to see your *actual* data. The initiative only gave consumers the right to see what *categories* of data had been collected about them, so this was a major, pro-consumer step forward.

b. Right to delete the information *you have posted.* Not as comprehensive as the European "Right to Erasure," but still, more than the initiative had.

c. Right to know the purposes for which a company is collecting your information. The initiative did not have this requirement.

d. Increased age from 13 to 16, prior to which companies must obtain 'opt-in' permission from the consumer before selling their data.

(2) Altered prohibition on not charging different prices if a consumer selects a privacy option.

a. The initiative had a total prohibition on any differential pricing—i.e. charging users for requesting that a company not share or sell their information.

b. The bill provides some flexibility on this point. Companies can charge consumers more if a consumer chooses not to have their data shared or sold, but:

i. Companies can only charge a differential that is *'directly related'* to the value of the consumer's data.[1]

ii. Companies must inform consumers and get opt-in consent to such a 'financial incentive' program (*i.e.,* if they 'pay' a consumer to allow his or her information to be sold).

iii. *Any such financial incentives cannot be unjust, unreasonable, coercive or usurious.* We think this requirement is critical in order to ensure a fair market solution.

c. In conclusion, CCPA as written provides flexibility to companies, but with transparency that will allow consumers to make informed decisions about which companies to do business with.

[1] Note that when the bill emerged from the Legislative Counsel's office, a typo was made, which both industry and privacy groups have committed to fixing in 2019. The existing language reads "A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data." In reality, it should read ". . . provided to the *business* by the consumer's data."

(3) Limited Private Right of Action

a. The initiative had enforcement by both the Attorney General, and a broad private right of action covering essentially all violations.

b. The law limits the private right of action to data breach violations, with penalties of from $100—$750 per violation.

c. The rest of the law is subject to Attorney General enforcement, at up to $2,500 per violation.

As proponent, it was my belief that the above compromise was the right one to make. The June passage of CCPA obtained many more consumer rights; it clarified a section with respect to pricing differently based on privacy choices; and it lessened the Private Right of Action, but kept substantial and meaningful penalties in place to ensure compliance.

GDPR vs CCPA: some major differences

Some have compared CCPA to the recently passed European General Data Protection Regulation. While there are conceptual similarities, the CCPA is significantly different.

The most obvious difference is in who is a covered entity: in Europe, all entities of any size are subject to GDPR, whereas CCPA only covers businesses with over $25M in revenue, and data brokers selling large amounts of personal information.

The second big difference is in the European approach of requiring user consent before *any* processing can take place.

Specifically, under GDPR, a corporation must obtain a consumer's approval before collecting and processing his or her data. The fact of notice and required consent prior to collection, is indeed a step towards greater respect for privacy, but we were concerned that given the massive pull and market share for some of the largest consumer-facing brands—think Google, or Facebook, or Amazon—the choice facing consumers to consent or not, was actually a false one, since most consumers would simply click "I agree" to the request for consent. [As it turns out, subsequent to GDPR's introduction, this concern has been validated [2]].

Additionally, and very importantly, we are concerned that this provision may hurt new entrants to the marketplace, since consumers may be unlikely to agree to the collection and sale of their information by a new entrant—so how does the *next* Google or Facebook even get off the ground?

As an alternative, if a consumer could restrict the sale of their information by any company he or she was doing business with, that felt like giving the consumer a more useful tool.

Current Status

At this point, the law is scheduled to go into effect on July 1, 2020. A "clean-up" bill, SB 1121, passed the legislature in August 2018, and despite efforts by the technology industry to substantially weaken key components of CCPA, our coalition was able to persuade the legislators to hold the line, and the law has remained substantially as intended when we agreed to a deal in June.

There will certainly be a battle in the coming years, either in the California Legislature or in Congress, as companies seek to return to a world free of any limitations on what they can do with consumers' personal information.

However, Californians for Consumer Privacy remains committed to ensuring that any bill passed in Sacramento or in Washington, contains at least the same protections for Californians, that they have so recently won.

Motivation Behind CCPA:

We live in a world where giant companies, the largest companies the world has ever known, are tracking us continually. We live in a world of commercial surveillance. During our research I became aware of the scale and scope of this surveillance, and include below some recent examples that have appeared in the press:

Google has a patent on using in-home [3] devices to track whether alcohol is being consumed; whether (and presumably, what kind of) smoking is taking place; whether teeth are being brushed, and for how long, and whether the water is being left running during the teeth-brushing. The patent extends to determining whether 'mischief' is occurring in the home, to determining the emotional state of the home's

[2] (Kostov, May 31 2018) *Google Emerges as Early Winner From Europe's New Data Privacy Law.* Wall Street Journal.

[3] Fadell, M., A., & al, e. (2016). United States Patent Application 20160261932. *US Patent Office.*

occupants (based on voice and facial expression), and to tracking whether foul language is being used.

Advertisers can erect "geofences" [4] *around any physical location or building*,[5] which are essentially just lines with latitudinal and longitudinal coordinates, and *can tag smartphones* [6] crossing such a fence, in order to send advertisements to that device. As a result, through no overt action of a consumer, the companies know who is in rehab, who goes to AA, *who just got* an abortion,[7] what your religion is, and whether you have a drug problem. If you're in rehab, or in jail, or go to an HIV clinic regularly, that information can be sold, and resold, simply because you have a mobile phone. This is the new reality—if the company can track your phone, they can track you.

Wearable activity monitors (think Fitbit) collect your most intimate data, and *none of it is covered by HIPAA until it reaches a doctor*,[8] hospital, or other covered entity—as a result much of it is available for *sharing or sale with third parties.*[9]

Employers can obtain information about their workforce from benefits managers,[10] who use sophisticated tools to figure out which employees might be trying to get pregnant, or be pre-diabetic; and in a small company with say only 20 women working, it is likely that if 10 percent of the workforce is trying to get pregnant, the manager knows who those two women are. Then, if the economy slows, and the manager needs to lay someone off . . . it might be easier to decide on the person who might be pregnant next year.

5 low-resolution images of your face are enough [11] [12] for an algorithm to determine your sexual orientation (91 percent confidence for men, 83 percent for women). And remember, there are 10 countries in the world *where to be gay is a crime punishable by death.*[13]

300 likes on Facebook are enough for an algorithm [14] to predict your answers to a well-established personality profile, better than even your spouse, and much better than your co-workers. If we're all looking for someone to truly understand us, what does it say when that person is . . . the algorithm?

Amazon has a patent to use photos taken in the home [15] to determine whether consumers are wearing certain images on their clothing (think a musician) and then using that to offer the consumer similar items for purchase.

China is monitoring consumers' behavior—who they associate with, what they search for, whether they jaywalk [16]—to *produce the famed* 'Social Credit' score.[17] [18] Combined with a comprehensive facial recognition system, this takes societal tracking and control to a new level—and yet, in what way does the Chinese government know less about its citizens, than the big search engines or social media companies know about Americans?

Anyone can purchase a list of *people taking certain medications*[19] or *police officers' home* addresses.[20] *Employers can easily advertise to only younger potential employees on* Facebook,[21] and do. *Racists can specifically target certain ethnic groups in*

---

[4] (White, November 1, 2017) *What is geofencing? Putting location to work.* CIO.

[5] (Copley, Last visited 10–2–18) *Geofencing—How it works [http://copleyadvertising.com/#how_works].* Copley Advertising Blog.

[6] (White, November 1, 2017) What is geofencing? Putting location to work. *CIO.*

[7] (Healey, 2017) Massachusetts Attorney General Press Release (2017). *AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities.*

[8] (Mobile Health and Fitness Apps: What Are the Privacy Risks?, Dec 16, 2016)

[9] (Fitbit and Google Partnership May Raise Privacy Concerns, May 25, 2018)

[10] (Picchi, February 18, 2016)

[11] (Levin, 9–7–17) *New AI can guess whether you're gay or straight from a photograph.* The Guardian.

[12] (Kosinkski, 5–12–2017) *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images.* PsyArXiv

[13] (Bearak, 6–16–2016) *Here are the 10 countries where homosexuality may be punished by death.* Washington Post.

[14] (Kosinksi, 1–27–2015) *Computer-based personality judgments are more accurate than those made by humans.* Proceedings of the National Academy of Sciences.

[15] (Maheshwari, March 31 2018) *Hey, Alexa, What Can You Hear? And What Will You Do With It?* New York Times.

[16] (Tracy, 4–24–2018) *China's social credit system keeps a critical eye on everyday behavior.* CBS News.

[17] (Rollet, June 5, 2018) *The odd reality of life under China's all-seeing credit score system.* Wired.

[18] (Larson, August 20 2018) *Who needs democracy when you have data?* MIT Technology Review.

[19] NextMark

[20] NextMark

[21] (Angwin, Dec 20, 2017) Dozens of Companies Are Using Facebook to Exclude Older Workers From Job Ads. *ProPublica.*

order to exclude them from renting an apartment,[22] or to try to get them *to join a hate group.*[23]

The majority of the world's websites have a Google,[24] [25] Facebook or Twitter tracker—so that your information is being sent back to those companies, and you are being tracked over the internet, wherever you go, using whatever device you're on.

And not just you: your children are being evaluated and tracked, often in direct contravention of laws like the Child Online Privacy Protection Act (COPPA), as was recently highlighted in a study showing almost 6,000 of the most popular children's Android[26] apps were potentially in violation of COPPA.

And not just online: in the physical world, *Google recently was in the news, and is now facing* multiple lawsuits, because it continued to track users up to 300 times *a day,*[27] even when the user had turned off his or her "location history," and seen this message in response *"You can turn off Location History at any time. With Location History off, the places you go are no longer stored."* However, despite the obvious implications of this message, Google continued to track users—and seemed to make it intentionally very difficult for even tech-savvy users trying to stop from being tracked, to turn off this constant location surveillance.

Consumers do not also generally understand that in many cases these businesses and apps allow partners to install a small piece of software or code on the user's smartphone, which allows that third party to track the user and collect all the information pertaining to his or her use of that app; and furthermore not just information about that user's interactions with the original app, but what other apps the user might have installed, or have open.

Weather apps are prime examples of this,[28] and many are in fact owned by data brokers, since consumers do not tend to turn off their location services for such apps, given it's more work to type in a zip code or a city, than to have the app simply display the weather forecast. But in so doing, they give the app real-time access to the consumer's exact location.

We call this whole suite of issues, the "expectation gap," *i.e.,* between what a user expects (that the app or company with which the consumer originally interacts, the "first party," will collect and process his/her data), and what actually happens (*i.e.,* that tens or hundreds of "third parties" the consumer has never heard of, suddenly get access to his or her interactions on their smartphone, and that his or her location is sold and resold).

A major part of the rationale behind CCPA, was to give consumers tools to deal with this "expectation gap."

CCPA is not anti-business. It was, on the contrary, written and proposed by businesspeople concerned that regulations were needed; that as in so many previous situations, whether of the giant trusts of a century and more ago, or of the telephone and related wiretapping concerns, or cigarettes and health, or autos and safety, this latest technology too, has outpaced society's ability to fully comprehend it yet, or its impact on all of us.

CCPA represents one step towards damming the flow of this river of information, from consumer towards giant, multinational corporation, and thence out to an entire ocean of companies the consumer has never heard of, and would never choose to do business with.

CCPA puts the focus on giving choice back to the consumer, a choice which is sorely needed.

The CHAIRMAN. Thank you, Mr. Mactaggart.

Ms. Moy.

---

[22] (Angwin, Facebook (Still) Letting Housing Advertisers Exclude Users by Race, Nov 21, 2017)

[23] (Angwin, Facebook Enabled Advertisers to Reach 'Jew Haters', Sept 14, 2017)

[24] (Simonite, May 18, 2016) *Largest Study of Online Tracking Proves Google Really Is Watching Us All.* MIT Technology Review.

[25] (Narayanan, 2016) *The Long Tail of Online Tracking.* Princeton Web Census.

[26] (Reyes, April 25, 2018) Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. Berkeley Laboratory for Usable and Experimental Security.

[27] (Tung, Aug 17, 2018) Google: To be clear, this is how we track you even with Location History turned off. *ZDNet.*

[28] (Mims, March 4, 2018) *Your Location Data Is Being Sold—Often Without Your Knowledge.* Wall Street Journal.

STATEMENT OF LAURA MOY, EXECUTIVE DIRECTOR, CENTER ON PRIVACY AND TECHNOLOGY, GEORGETOWN LAW

Ms. MOY. Thank you.

Good morning, Chairman Thune. Good morning, Senator Markey, and members of the Committee.

I am very grateful for the opportunity to present before this Committee today.

I wanted to start with a little context. I am not here today because I am worried about private information being made public. And although this is about the classic right to be left alone, outlined by Brandeis and cited just a moment ago in this hearing, this is also about the need to grapple with the implications of unbridled data collection, storage, processing, and use; things that give those who wield data more power to influence society than we could have imagined before the Digital Era.

This is about confronting the ways in which the data driven economy is contributing to extreme wealth disparity, extreme political polarization, extreme race and class-based tension, and extreme information manipulation.

This is not a time to be shy about data regulation. It is not a time for "light touch" regulation, which has already been tried and has led us to where we are today. Now is the time to intervene, and I thank you all for having this hearing. Here is where we should start.

First, we should agree that there are things information simply should not be used for. Chief among these is discrimination. Information that Americans share online should not be used to selectively deny them access to, or awareness of, things like housing, education, finance, employment, and health care. Data should be used to increase opportunities, not to stifle them.

Americans' information also should not be used to amplify hate speech or to enable data brokers to build ever more detailed profiles of us that they then turnaround and sell to the highest bidder. It should not be used to target misinformation and disinformation that compromises our social fabric.

Notice and choice are good when notice is understandable and the choice truly is a choice, but it is not enough.

Second, we need robust enforcement. Congress must empower an expert agency to vigorously enforce the law including with the ability to levy substantial fines against companies that violate their data obligations.

In fact, staff and commissioners of the Federal Trade Commission have appeared before Congress directly requesting this authority. State attorneys general should also be empowered to enforce privacy.

A single agency cannot hope to police the entire digital ecosystem. State attorneys general do indispensable work both enforcing privacy laws and providing valuable guidance to companies trying to comply with the law.

Congress should also consider creating a private right of action so that individual people can protect their own privacy when enforcement agencies do not.

Third, we need a way to make sure the law will keep up with changing technology. We cannot know what the next privacy or

data security threat will be, but what we do know unfortunately is that there will be one. That is why any new privacy law must include a mechanism for updating standards to respond to shifting threats. The best way to do this is to pass a Federal law that creates a floor, not a ceiling, for privacy so that states can continue to pass stronger laws on their own as they are doing.

Privacy and data security are extremely active issue areas for states, which are, after all, our laboratories of democracy.

We should also have robust rulemaking authority for an expert agency. A regulatory agency can respond to rapidly changing technology more quickly than Congress.

Fourth, we should not attempt to address complex challenges with a "one size fits all" approach. There are different types of actors on the Internet with different roles to play, different relationships with and commitments to users, different competition environments, and different abilities to solve problems.

Industry has called for regulatory uniformity. That has a nice sound to it, but if we adopt a uniform approach to the entire Internet, I fear that we may be left with the lowest common denominator, something that looks like transparency with enforcement that just prohibits deceptive practices. We already have that and it has proven not enough. Americans are asking for more.

Thank you and I look forward to your questions.

[The prepared statement of Ms. Moy follows:]

PREPARED STATEMENT OF LAURA MOY, EXECUTIVE DIRECTOR, CENTER ON PRIVACY & TECHNOLOGY, GEORGETOWN LAW

Introduction and Summary

Chairman Thune, Ranking Member Nelson, and Members of the Committee, thank you for inviting me here today. I am Laura Moy, executive director of the Center on Privacy & Technology at Georgetown Law. I appreciate the opportunity to testify on consumer privacy.

It feels significant to come before this institution in such an electrically charged time, and it feels important to speak truth in that context. So I wanted to start by explaining why I am here. I am not here today because I am worried about private information being made public. This is not, for me, just about the classic "right to be left alone."

This is about our country—and the world—grappling with the implications of unbridled data collection, storage, and use—things that give the holders and users of data more power to influence society than we could have imagined before the digital era. This is about confronting the ways in which the data-driven economy is contributing to extreme wealth disparity, extreme political polarization, extreme race-and class-based tension, and extreme information manipulation. We need to come together to rein in the problematic ways in which Americans' data is being collected and stored without meaningful limitations, and used in ways that harm not only individuals, but our broader society.

As this Committee considers what form those solutions might take, I offer a handful of recommendations that I hope to highlight in my testimony today:

- *First, there are appropriate and inappropriate collections and uses of Americans' information.* To foster data fairness, baseline obligations should attach to all collections and uses of consumer data. And some applications for Americans' data should simply be off-limits. Chief among these is discrimination—information should not be used to selectively deny access to—or awareness of—critical opportunities in housing, education, finance, employment, and healthcare.
- *Second, privacy protections should be strongly enforced by an expert agency.* Standards are only as strong as their enforcement, so whatever standards this legislature crafts, they should be enforceable by an expert agency that has civil penalty authority and sufficient staff, resources, and motivation to get its job done.

- *Third, privacy protections should also be enforced by state attorneys general.* Federal agencies cannot possibly hope to police the entire digital ecosystem. State attorneys general are already doing extensive and excellent work on privacy and data security, and they must be empowered to continue to do that good work under any new legislation.
- *Fourth, privacy and data security protections should be forward-looking and flexible.* As the technological landscape changes, privacy and data security standards must constantly be updated. State legislatures are already doing this, operating as the "laboratories of democracy" they are supposed to be, and Federal law should not hamstring states' ability to continue to do this work. Any new standards on privacy and data-security standards should also include rulemaking authority for an expert agency that is able to keep abreast of and respond to shifting threats as technology advances.
- *Fifth, protections for Americans' private information should take into account the context in which information is shared.* There are different types of actors on the Internet with different roles to play, different relationships with and commitments to users, different competition environments, and different abilities to solve problems. Any new privacy and data security standards should be tailored to ensure that Americans continue to benefit from heightened privacy standards in contexts in which choices are limited and privacy expectations are higher.
- *Sixth, Congress should not eliminate existing protections for Americans' information.* This should go without saying, but as Congress considers establishing new privacy and data security protections for Americans' private information, what it should *not* do is eliminate existing protections that are already benefiting Americans in state or other Federal laws.

1. We need to broaden the conversation on privacy

"Privacy" has many definitions. For example, it could refer to the right to keep private information from being exposed to the public, the right to control information about oneself, the right to be left alone, the right to ensure that information is used and shared in a way that is consistent with norms and expectations, or the right to prevent information from being transferred to those who would use it to do harm. It is all of these things, but in the networked era it is more.

When we talk about privacy today, we should also be thinking about the right to ensure that our information is not used in ways not only that harm ourselves, but that harm society as a whole. For example, beyond subjecting individual users to specific uses and transfers that they find objectionable, information uses and misuses may harm society by:

- Chilling both adoption and free and open use of the internet. The FCC concluded in the 2010 *National Broadband Plan* that concerns about online privacy and security "may limit [consumers'] adoption or use of broadband."[1] More recently, NTIA reported that 45 percent of households limited their online activities because of privacy and security concerns.[2]
- Undermining trust in the digital environment. When information is not sufficiently protected, Americans cannot fully trust the digital environment. But as privacy scholars writing on the importance of trust as an element of privacy policymaking have explained, "trust drives commerce and it creates the conditions for intimacy and free expression. If we want to flourish as humans, we must be able to trust each other."[3]
- Supporting the dissemination of propaganda, misinformation, and disinformation. Americans' data may be used to generate and target false information, including state-sponsored propaganda, careless or low-quality reporting, and false information designed and intended to undermine democracy.[4] As false information proliferates, Americans are rapidly losing trust in journalism.

---

[1] FCC, *Connecting America: The National Broadband Plan* 17 (2010), *https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.*

[2] Rafi Goldberg, NTIA, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities* (May 13, 2016), *https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.*

[3] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law,* 19 Stan. Tech. L. Rev. 431, 456 (2016).

[4] David McCabe, *Facebook Finds New Coordinated Political Disinformation Campaign,* Axios, July 31, 2018, *https://www.axios.com/facebook-finds-misinformation-campaign-4c5910b3-021a-45b7-b75c-b1ac80cbce49.html;* Dipayan Ghosh & Ben Scott, *Disinformation Is Becoming Unstoppable,* Time, Jan. 24, 2018; April Glaser & Will Oremus, *The Shape of Mis- and Disinformation,* Slate, July 26, 2018, *https://slate.com/technology/2018/07/claire-wardle-speaks-to-if-then-*

- Amplifying hate speech. Americans' data may also be used to make the distribution of hateful and racist rhetoric and calls to violence more efficient.[5]
- Driving political polarization. Americans' data may also be used to drive content distribution platforms that are more likely to promote hyper-partisan content, which in turn may exacerbate political polarization. As one prominent legal scholar has written, "Self-insulation and personalization are solutions to some genuine problems, but they also spread falsehoods, and promote polarization and fragmentation."[6]
- Damaging public health. Digital sites and services often use users' data to inform design choices that will increase user engagement, including by intentionally designing products to be addictive and inescapable.[7] This can lead to a cascade of other problems, including heightened rates of depression, suicide, and sleep deprivation among young people.[8]

We should be thinking of these problems as we consider how best to approach data legislation in the 21st century. It may not be possible to solve all of these problems at once, but any proposed legislative solution to one problem should be scrutinized to ensure that it does not inadvertently make these problems worse, or hamper the ability of states or enforcement agencies to innovate additional approaches to some of these problems moving forward.

2. We must do better on privacy

We must do better on privacy. Americans consistently are asking for policymakers to step in. 91 percent of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies, and 68 percent believe current laws are not good enough in protecting people's privacy online. In response to one 2015 survey, 80 percent of respondents were "concerned" or "very concerned" when asked about their online privacy.[9] For years, consumers have been expressing concern and even anger about the way their personal information is collected and used without their control, consent, or even knowledge.[10] Americans feel powerless to regain control over their privacy—in the modern era, Internet access is necessary for employment, education, access to housing, and full participation in economic and civic life.

In the absence of robust regulation, although providers of online sites and services often engage in ongoing conversations with civil rights, civil liberties, and public interest groups, they nevertheless have repeatedly failed to respect and protect data relating to millions—and at times billions—of users. For example, despite repeated assurances to regulators, the public, and advocates that it would protect consumer privacy, Facebook has revealed breach after massive breach, including when, less

---

about-how-disinformation-spreads-on-social-media.html; Alice Marwick & Rebecca Lewis, *Media Manipulation and Disinformation Online* (2017), *https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.*

[5] *See* Ariana Tobin, Madeleine Varner, & Julia Angwin, *Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up,* ProPublica, Dec. 28, 2017, *https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes;* Swathi Shanmugasundaram, Southern Poverty Law Center, *The Persistence of Anti-Muslim Hate on Facebook* (May 5, 2018), *https://www.splcenter.org/hatewatch/2018/05/05/persistence-anti-muslim-hate-facebook.*

[6] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* at 5 (2017).

[7] Center for Humane Technology, The Problem, *http://humanetech.com/problem/* (last visited Oct. 7, 2018) (explaining that operators of online services competing for users' attention are constantly learning how better to "hook" their users, and designing products intentionally to addict users).

[8] Recent studies have linked the use of platforms like Facebook, Snapchat, and Instagram to depressive symptoms in young adults caused by negatively comparing oneself to others on social media platforms. Brian A. Feinstein, *et al., Negative Social Comparison on Facebook and Depressive Symptoms: Rumination as a Mechanism,* 2 Psych. Pop. Media Culture 161 (2013). *http://psycnet.apa.org/record/2013-25137-002.* Experts have also found that teens who spend three hours a day or more on electronic devices are 35 percent more likely to have a risk factor for suicide and 28 percent more likely to get less than seven hours of sleep. Jean M. Twenge, *Have Smartphones Destroyed a Generation?,* The Atlantic, Sept. 2017, *https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198/.*

[9] Freedman Consulting, *Poll Finds Strong Support for Expanding Online Privacy Protections and Internet Access* (Nov. 23, 2015), available at *https://www.freedmanconsulting.com/documents/PrivacyandAccessResearchFindings_151123.pdf.*

[10] Lee Rainie & Maeve Duggan, Pew Research Center, *Privacy and Information Sharing* 2 (Jan. 14, 2016), *http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf* ("In online focus groups and in open-ended responses to a nationally representative online survey, many people expressed concerns about the safety and security of their personal data in light of numerous high-profile data breaches. They also regularly expressed anger about the barrage of unsolicited e-mails, phone calls, customized ads or other contacts that inevitably arises when they elect to share some information about themselves.").

than two weeks ago, it announced a breach that may have affected up to 90 million users.[11] Last year data miners, chief among them Cambridge Analytica, successfully used Facebook's platform to learn private information about many more than 87 million users.[12] And Facebook also recently revealed that "malicious actors" had exploited search tools on its platform to harvest profile details of most of its two billion users.[13] Despite Google's past promises to stop scanning the inboxes of Gmail users for information to target marketing, it was reported in July that the company continues to let hundreds of third-party companies scan the inboxes of millions of Gmail users, doing little to police what those third parties do with users' information.[14] Google also revealed that it still tracks users' location through use of its services even after users have disabled the "Location History" feature.[15] And the past several months have seen major security breaches affecting, among others, Orbitz,[16] Under Armour,[17] Ticketfly,[18] and British Airways.[19]

Consumers are outraged and consistently are calling for greater oversight and accountability. Consumers should be able to trust that when they go online, their information will not be used to harm them.

3. Recommendations for the Committee as it considers how to address privacy

It is in this context—when Americans are increasingly concerned about privacy, and when the stakes are higher than ever—that this Committee is grappling with these many complex and important issues. Now is not the time to be shy about stepping in. "Light-touch" regulation has already been tried, and it has led us to the predicament we find ourselves in today. To sufficiently protect Americans from harmful uses of their data, much more must be done. Below, I offer a handful of recommendations to this Committee about where to begin.

A. Recognize that there are appropriate and inappropriate collections and uses of Americans' data

It is long past time for us to move beyond a privacy framework built on the concept of notice and choice, and to recognize that there should be minimum criteria that determine when collection and use of information is appropriate, and there are also things information simply should not be used for. As the digital era advances, notice is becoming less and less meaningful—it is increasingly difficult for consumers to understand the many ways in which their information might be collected, what that information might reveal about them, and how it might be used. And "choices" often are not true choices. Americans don't feel that they have a choice about whether or not to go online—and because we all recognize that an online presence is indispensable in the 21st century, we don't want them to treat it like a

---

[11] Louise Matsakis & Issie Lapowsky, *Everything We Know About Facebook's Massive Security Breach,* WIRED, Sept. 28, 2018, *https://www.wired.com/story/facebook-security-breach-50-million-accounts/*.

[12] Alex Hern, *Far More than 87m Facebook Users Had Data Compromised, MPs Told,* The Guardian, Apr. 17, 2018, *https://www.theguardian.com/uk-news/2018/apr/17/facebook-users-data-compromised-far-more-than-87m-mps-told-cambridge-analytica.*

[13] Craig Timberg, Tony Romm, & Elizabeth Dwoskin, *Facebook: 'Malicious Actors' Abused Its Search Tools to Collect Data on Most of Its Two Billion Users,* The Independent, Apr. 5, 2018, *https://www.independent.co.uk/news/world/americas/facebook-hackers-personal-data-collection-users-cambridge-analytica-trump-mark-zuckerberg-latest-a8289816.html*

[14] Douglas MacMillan, *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail,* WSJ, July 2, 2018, *https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442.*

[15] Chaim Gartenberg, *Google Updated its Site to Admit It Still Tracks You Even if You Turn Off Location History,* The Verge, Aug. 17, 2018, *https://www.theverge.com/2018/8/17/17715166/google-location-tracking-history-weather-maps.*

[16] Robert Hackett, *Expedia's Orbitz Says Data Breach Affected 880,000 Payment Cards,* Forbes, Mar. 20, 2018, *http://fortune.com/2018/03/20/expedia-orbitz-data-breach-cards/*.

[17] Hamza Shaban, *Under Armour Announces Data Breach Affecting 150 Million MyFitnessPal Accounts,* Wash. Post, Mar. 29, 2018, *https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/under-armour-announces-data-breach-affecting-150-million-myfitnesspal-app-accounts/*.

[18] Travis M. Andrews, *Ticketfly is Back Online After a Hack Exposed About 27 Million Accounts. Here's What You Need to Know.,* Wash. Post, June 7, 2018, *https://www.washingtonpost.com/news/arts-and-entertainment/wp/2018/06/05/ticketfly-has-been-hacked-heres-what-you-need-to-know/*.

[19] Ivana Kottasová, *British Airways' Latest Tech Problem Is a Major Credit Card Hack,* CNN Business, Sept. 7, 2018, *https://money.cnn.com/2018/09/07/investing/ba-hack-british-airways/index.html.*

choice, and avoid going online. Nor do consumers have a true choice about whether or not to share their information with a number of entities they encounter online.[20]

Beyond notice and choice, legislation should define baseline obligations that automatically attach when Americans' information is collected or used. Those obligations should be based on the familiar Fair Information Practices (FIPs) of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[21] The FIPs framework creates meaningful obligations for companies that collect personal data, and rights for individuals whose personal data is collected.

Legislation should also inhibit uses of data that simply should not be allowed. Chief among these is discrimination. The information that Americans share online should not be used to selectively deny them access to—or awareness of—critical opportunities, especially things like housing, education, finance, employment, and healthcare. It should not be used to amplify hate speech. It should not be used to enable data brokers to secretly build ever-more-detailed profiles of us that they then turn around and sell, unrestricted, to the highest bidder.

At present, these impermissible uses of information are widespread. For example, on discrimination, Facebook made assurances in 2017 to tackle discriminatory advertising on its platform after facing public outrage and pressure from advocates regarding its "ethnic affinity" advertising clusters, but the Washington State Attorney General found that it was still possible to exclude people from seeing advertisements based on protected class membership.[22] Civil rights organizations are also suing Facebook for enabling landlords and real estate brokers to exclude families with children, women, and other protected classes of people from receiving housing ads,[23] as well as for gender discrimination on job ads.[24] And the systematic targeting and exclusion of communities can also be a byproduct of algorithmic content and ad distribution that optimizes for cost-effectiveness and user "engagement," which can lead to distribution that is discriminatory in impact, if not intent.[25]

Any new privacy legislation should establish standards that attach substantive legal obligations to collection and use of consumers' data, and that protect Americans from the most harmful uses of their information.

B. Privacy protections should be strongly enforced by a Federal expert agency

Privacy standards are only as strong as their enforcement. Congress must empower an expert agency to vigorously enforce the law—including with the ability to fine companies for privacy and data security violations. At present, although the Federal Trade Commission is expected to enforce the privacy promises of most of the commercial sector, with few exceptions, the agency does not have the ability to

---

[20] For example, consumers have no choice about whether or not to share information with a broadband provider in order to go online—and in many places in the country, there is only one choice of provider when it comes to high-speed broadband. Consumers also have virtually no choice about whether to share information with either Apple or Google when selecting an internet-enabled smartphone, virtually no choice about whether to share information with pervasive analytics and advertising networks, and, in some cases, no choice about whether or not to engage with social media platforms. In some instances, employers even require employees to have social media accounts.

[21] *See* Int'l Ass'n Privacy Professionals, *Fair Information Practices, https://iapp.org/resources/article/fair-information-practices/* (last visited Oct. 7, 2018); Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm* (last visited Oct. 7, 2018).

[22] Sam Machkovech, *Facebook Bows to WA State to Remove "Discriminatory" Ad Filters,* Ars Technica, July 25, 2018, *https://arstechnica.com/information-technology/2018/07/facebook-bows-to-wa-state-pressure-to-remove-discriminatory-ad-filters/*.

[23] Nat'l Fair Housing Alliance, *Facebook Sued by Civil Rights Groups for Discrimination in Online Housing Advertisements* (Mar. 27, 2018), *https://nationalfairhousing.org/2018/03/27/facebook-sued-by-civil-rights-groups-for-discrimination-in-online-housing-advertisements/*.

[24] Communications Workers of America, *CWA Sues Facebook for Gender Discrimination on Job Ads* (Sept. 20, 2018), *https://www.cwa-union.org/news/cwa-sues-facebook-for-gender-discrimination-on-job-ads.*

[25] *See* Anja Lambrecht & Catherine E. Tucker, *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads* (Mar. 9, 2018), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260* (finding that because younger women are an expensive demographic to show ads to, "An algorithm which simply optimizes cost-effectiveness in ad delivery will deliver ads that were intended to be gender-neutral in an apparently discriminatory way, due to crowding out."); Latanya Sweeney, *Discrimination in Online Ad Delivery,* Communications of the ACM, May 2013, at 44, *https://cacm.acm.org/magazines/2013/5/163753-discrimination-in-online-ad-delivery/*.

levy fines for privacy and data security.[26] This is widely viewed as a challenge by agency officials; indeed, civil penalty authority has been explicitly requested by multiple FTC officials, including Chairman Simons, Commissioner Slaughter, former Commissioner Ohlhausen, former Commissioner Terrell McSweeny, and former Director of the Bureau of Consumer Protection, Jessica Rich.[27] To improve privacy and data security for consumers, the FTC—or another agency or agencies—must be given more powerful regulatory tools and stronger enforcement authority.

Agencies also need resources to do their jobs well. The FTC is a relatively small agency, and should be given additional staff and resources if it is to be expected to step up its work on privacy. The agency has a small Office of Technology Research and Investigation (OTech), but would benefit from a larger Bureau of Technology equipped to fully grapple with the challenges of advancing technology—an idea supported by numerous current and former FTC officials.[28] An agency expected to enforce the privacy and security obligations of companies that do business in a digital world should be vested with the necessary expertise and resources to do that job well.

Even with additional staff and resources, however, enforcement agencies may, for a variety of reasons, sometimes fail to strongly enforce privacy standards.[29] To provide an additional backstop for consumers in the event that agencies lack the capacity or motivation to effectively enforce, Congress should also consider granting individual consumers themselves the right to bring civil actions against companies for violating privacy regulations.

---

[26] There are exceptions to this rule. As the FTC explains, "If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule." FTC, *Privacy & Security Update 2016, https://www.ftc.gov/reports/privacy-data-security-update-2016.*

[27] *See, e.g.,* Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (calling for civil penalty authority, arguing that monetary penalties "would actually . . . cause the business to think through how it's conducting . . . its business and what it's doing in terms of security and privacy."); *id.* (statement of Rebecca Kelly Slaughter, Commissioner, Fed. Trade Comm'n) (calling for civil penalty authority); Maureen Ohlhausen, Commissioner, Fed. Trade Commission, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), transcript available at *https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf;* Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?,* 2 Geo. L. Tech. Rev. 514, 529 (2018), *https://www.georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-McSweeny-pp-514–30.pdf; Opportunities and Challenges in Advancing Health Information Technology: Hearing Before the Subcomms. on Info. Tech. and Health, Benefits, and Admin. Rules of the H. Oversight and Gov't Reform Comm.* (2016) (statement of Jessica Rich, Director of the Bureau of Consumer Protection, Fed. Trade Commission).

[28] A Bureau of Technology is an idea that has been cited by Chairman Joseph Simons, Commissioner Rebecca Kelly Slaughter, former Commissioner Terrell McSweeny, and Professor David Vladeck, former Director of the Bureau of Consumer Protection. *See, e.g.,* Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (stating that the Commission is "affirmatively evaluating whether to create a bureau of technology"); McSweeny, *supra* note 27, at 530; U.S. Fed. Trade Comm'n, *Remarks of Commissioner Rebecca Kelly Slaughter on Raising the Standard: Bringing Security and Transparency to the Internet of Things?* at 5 (July 26, 2018), *https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter_-_raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf;* Aaron Fluitt, Institute for Technology Law & Police at Georgetown Law, *Georgetown's David Vladeck Outlines Challenges and Opportunities for Incoming FTC Commissioners* (Apr. 6, 2018), *https://www.georgetowntech.org/news-fullposts/2018/4/7/april-6-2018-georgetowns-david-vladeck-outlines-challenges-opportunities-for-incoming-ftc-commissioners.*

[29] The FTC has come under criticism for not doing enough to enforce its consent decrees. *See* Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation,* Techonomy, May 4, 2018, *https://techonomy.com/2018/05/facebook-whatsapp-lesson-privacy-protection-necessary-innovation/.* And the FCC has been widely criticized for not doing enough to protect security and privacy of phone users. *See* Craig Timberg, *How Spies Can Use Your Cellphone to Find You—and Eavesdrop on Your Calls and Texts, Too,* Wash. Post, May 30, 2018, *https://www.washingtonpost.com/business/technology/how-spies-can-use-your-cellphone-to-find-you-and-eavesdrop-on-your-calls-and-texts-too/2018/05/30/246bb794-5ec2-11e8-a4a4-c070ef53f315_story.html; Wyden Demands FCC Investigate Unauthorized Tracking of Americans' Cell Phones* (May 11, 2018), *https://www.wyden.senate.gov/news/press-releases/wyden-demands-fcc-investigate-unauthorized-location-tracking-of-americans-cell-phones;* Violet Blue, *FCC Shrugs at Fake Cell Towers Around the White House,* Engadget, June 8, 2018, *https://www.engadget.com/2018/06/08/fcc-shrugs-at-fake-cell-towers-around-the-white-house/.*

C. Privacy protections should also be enforced by state attorneys general

State attorneys general should also be empowered to enforce privacy. A single agency cannot hope to police the entire digital ecosystem. State attorneys general do a large volume of important work in this area, both enforcing privacy laws and providing valuable guidance to companies trying to comply with the law.

Attorneys general frequently provide companies with ongoing guidance to help businesses understand, adapt to, and comply with legal requirements and best practices. As explained by scholar Danielle Citron, who wrote about the importance of state attorneys general in developing privacy standards,

> Attorneys general establish task forces with business leaders, advocacy groups, and experts in the hopes that participants reach consensus on best practices. They reach out to companies with concerns about products and services. Staff provide advice to companies.[30]

The guidance provided by state attorneys general is vitally important. For example, in 2012 Vermont Attorney General William Sorrell partnered with a local university to offer free penetration tests to businesses to help them identify basic security vulnerabilities.[31] Speaking at an event the following year, Sorrell said it was important to his office to create a collaborative working relationship with companies. "If we find vulnerability, we tell the company," he said.[32] That program was later integrated into the services of the recently-established Vermont Agency of Digital Services.[33]

State attorneys general also generate best practice guides. According to Citron,

> In preparing guides, staff consult with stakeholders from a broad range of interests . . . Stakeholder meetings can involve dozens of participants: the goal is to get as many perspectives as possible. AG offices educate stakeholders about best practices.[34]

If Federal agencies are given the extra authority and resources they desperately need to do more privacy and data security work, they will be better able to address large privacy and data security cases, but will still be overwhelmed without the complementary consumer protection support of state attorneys general in thousands of small cases each year.[35]

To ensure that consumers receive the best protection they possibly can, state attorneys general must be given the ability to help enforce any new Federal standard. This type of authority exists—and has been successful—under the Children's Online Privacy Protection Act.[36]

D. Protections for Americans' private information should be forward-looking and flexible

Any new legislation on privacy and/or data security must also be designed to be forward-looking and flexible, with built-in mechanisms to foster regulatory agility. We do not know what the next privacy or data security threat is going to be, but plainly there will be one, and it will arise faster than Congress will be able to react.

---

[30] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General,* 92 Notre Dame L. Rev. 747, 759 (2016).

[31] *See id.*

[32] Paul Shukovsky, *State Attorneys General Are Crucial Force in Enforcement of Data Breach Statutes,* Bloomberg Law: Privacy & Data Security, Oct. 7, 2013, *https://www.bna.com/state-attorneys-general-n17179877665/*.

[33] *See* Vermont Agency of Digital Services, *Security Services http://dii.vermont.gov/infrastructure/security* (last visited Oct. 7, 2018).

[34] Citron, *supra* note 30, at 760.

[35] For example, according to the Massachusetts State Attorney General's Office, Massachusetts alone saw 2,314 data breaches reported in 2013, 97 percent of which involved fewer than 10,000 affected individuals. *Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Energy & Commerce Comm.* (2015) (statement of Sara Cable, Assistant Att'y Gen., Office of Mass. State Att'y Gen.). Each data breach affected, on average, 74 individuals. *Id.*

[36] The Children's Online Privacy Protection Act enables state attorneys general to bring actions on behalf of residents of their states against operators of online sites or services that they believe have violated children's privacy regulations. 15 U.S.C. §6504. State attorneys general use this authority; indeed, just weeks ago, the State Attorney General of New Mexico filed a suit against several companies for alleged children's privacy violations. *See AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data* (Sept. 12, 2018), *https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location_Personal_Data_1.pdf.*

Any broad privacy law must therefore include a mechanism for updating standards in accordance with shifting threats.

The need for regulatory agility is currently being met by state legislatures. In recent years, not only has California passed the California Consumer Privacy Act,[37] but Vermont passed the Data Broker Act,[38] and between 2015 and 2018 at least 23 different states—from all regions of the country—passed data security or breach notification legislation.[39]

Given the high level of legislative activity currently taking place at the state level on these issues, the most straightforward way to preserve regulatory flexibility in privacy and data security would be simply to leave state legislative authority intact. To do this, new Federal legislation should establish a floor, not a ceiling for privacy—thus allowing states to continue to pass stronger laws on their own. States will no doubt continue to actively use this authority, as they are already doing.

As an additional measure to support regulatory agility, any agency or agencies that are to be tasked with protecting the privacy and security of consumers' information should be given rulemaking authority. Indeed, FTC commissioners have directly asked Congress for rulemaking authority.[40]

Rulemaking enables agencies to adjust regulations as technology changes, as the FTC did just a few years ago with the COPPA Rule.[41] As a starting point, the FTC should be given rulemaking authority over data security, data brokers, and consumer privacy.

E. Protections for Americans' private information should take into account the context in which information is shared

There is no one-size-fits-all approach for privacy. Rather, privacy standards often must be context-specific, carefully tailored based on the avoidability of the information sharing, the sensitivity of the information shared, and the expectations of consumers. As it considers establishing comprehensive baseline privacy standards, Congress should therefore not assume that existing privacy laws should simultaneously be eliminated. Many of those existing narrower privacy laws have already been appropriately tailored to establish heightened privacy standards under specific circumstances, in accordance with important contextual considerations relating to unavoidability and sensitivity.

First, heightened standards should apply when information sharing is unavoidable or less avoidable by consumers. This is consistent with several existing laws that protect consumer information in specific contexts in which sharing is unavoid-

---

[37] California Consumer Privacy Act, *https://www.caprivacy.org/* (last visited October 7, 2018).

[38] Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers,* TechCruch, May 27, 2018, *https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/*.

[39] Since 2015, data security or breach notification legislation has been enacted in Alabama, Arizona, California, Connecticut, Delaware, Florida, Illinois, Iowa, Maryland, Montana, Nebraska, New Hampshire, New Mexico, North Dakota, Oregon, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, and Wyoming. *See* Nat'l Conf. State Legislatures, *2015 Security Breach Legislation* (Dec. 31, 2015), *http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx;* Nat'l Conf. State Legislatures, *2016 Security Breach Legislation* (Nov. 29, 2016), *http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx;* Nat'l Conf. State Legislatures, *2017 Security Breach Legislation* (Dec. 29, 2017), *http://www.ncsl.org/research/telecommunications-and-information-technology/2017-security-breach-legislation.aspx;* Natl' Conf. State Legislatures, *2018 Security Breach Legislation, http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx* (last visited Oct. 7, 2018).

[40] Maureen K. Ohlhausen, FTC Commissioner, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), available at *https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf* ("Legislation in both areas—data security and breach notification—should give the FTC . . . rulemaking authority under the Administrative Procedure Act"); *Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (stating he "support[s] data security legislation that would give . . . the authority to issue implementing rules under the Administrative Procedure Act"); *id.* (statement of Rebecca Kelly Slaughter, Comm'r) (calling for APA rulemaking authority); *id.* (statement of Rohit Chopra, Comm'r) (also supporting rulemaking authority, stating, "the development of rules is a much more participatory process than individual enforcement actions and it also gives clear notice to the marketplace rather than being surprised, and I think it would be a good idea.").

[41] Federal Trade Commission, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Amending Children's Online Privacy Protection Rule* (Dec. 19, 2012), *https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.*

able—such as the information shared by students in an educational context,[42] by consumers in a financial context,[43] by customers in a telecommunications context,[44] and by patients in a medical context.[45]

This is also consistent with the FTC's evaluation of potentially problematic data-related practices under its Section 5 authority to prohibit unfair practices. When considering whether a practice is unfair, the FTC asks not only whether the practice is harmful, but also whether the practice is one that consumers can avoid. In its policy statement on unfairness, the FTC explained,

> Normally we expect the marketplace to be self-correcting, and we rely on consumer choice—the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.[46]

Whether or not information sharing is avoidable by a consumer is often tied to the question of whether or not a service or transaction is essential. When a service is essential—such as with phone service—information sharing may be considered unavoidable because the consumer cannot reasonably decline the service altogether. This, too, helps explain why heightened privacy protections apply in the educational,[47] financial,[48] telecommunications,[49] and medical contexts—all of these contexts involve essential services.[50]

Heightened standards also should apply in contexts in which the information shared or typically shared is sensitive. For example, the Children's Online Privacy Protection Act recognizes that information about children deserves heightened protection.[51] Other laws recognize the heightened sensitivity of health information[52] and financial information.[53] In the past, the question of sensitivity has often been the most important in considering how well the law should protect consumers' information. Data analysis techniques have advanced over time, however, and it is becoming clear that classically sensitive information can often be deduced from categories of information not traditionally thought of as sensitive. For example, as computer scientist Ed Felten explained in testimony before the Senate Judiciary Committee regarding telephone metadata, "Calling patterns can reveal when we are awake and asleep; our religion . . . our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations."[54] In 2016 the FTC found that television viewing history can be considered sensitive information,[55] and the Federal Communications Commission (FCC) found that web brows-

---

[42] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[43] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[44] 47 U.S.C. § 222.
[45] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104– 191, 110 Stat. 1936 (1996).
[46] FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), *https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.*
[47] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[48] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[49] 47 U.S.C. § 222.
[50] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104– 191, 110 Stat. 1936 (1996).
[51] 15 U.S.C. §§ 6501–6506.
[52] *E.g.* Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).
[53] *E.g.* Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[54] *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing before the S. Comm. on the Judiciary,* 113th Cong. 8–10 (2013) (statement of Edward Felten, Prof. of Computer Science and Public Affairs, Princeton Univ.).
[55] Complaint at ¶ 32, *FTC v. Vizio,* Case No. 2:17-cv-00758, D.N.J. (filed Feb. 6, 2017), available at *https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.*

ing history can be considered sensitive.[56] Indeed, patent applications filed by Google indicate that it is possible to estimate user demographics and location information based on browsing histories.[57]

F. Congress should not eliminate existing protections for Americans' information

Finally, as Congress considers establishing new privacy and data security protections for Americans' private information, it should not eliminate existing protections that already benefit Americans under state or other Federal laws. Americans are asking for *more* protections for their private information, not less. This explains why consumers—on both sides of the aisle—were outraged when Congress voted last year to eliminate strong privacy regulations that had been passed by the FCC.[58] Some lawmakers argued that repeal of the FCC's rules was needed to foster development of a consistent approach to privacy across the Internet.[59] But as FTC Commissioner Terrell McSweeny noted, "If consistency were truly the goal, then we would likely increase protections for privacy, rather than unraveling them. That is the policy conversation we ought to be having—instead we are fighting a rear-guard action defending basic protections."[60]

Congress also should not eliminate existing and future consumer protections at the state level. As noted above, state laws play an important role in filling gaps that exist in Federal legislation. For example, a number of states have expanded the scope of their data security and breach notification laws to extend protections to previously unregulated market sectors and private data—and consumers in those states are benefiting from those existing laws. For example, Connecticut's data security and breach notification statute covers entities operating at multiple nodes of the health care pipeline.[61] California adopted a data security statute—the Student Online Personal Information Protection Act (SOPIPA)—that is tailored to online educational platforms.[62] SOPIPA prompted twenty-one other states to adopt student data security laws modeled on California's example.[63] Minnesota adopted a law requiring Internet Service Providers (ISPs) to maintain the security and privacy of consumers' private information.[64] And Texas now requires any nonprofit athletic or sports association to protect sensitive personal information.[65]

Some states have also expanded the types of information that data holders are responsible for protecting from unauthorized access, or for notifying consumers of when breached. For example, ten states have expanded breach notification laws so that companies are now required to notify consumers of unauthorized access to their biometric data—unique measurements of a person's body that can be used to determine a person's identity.[66] This important step recognizes that a biometric identifier such as a fingerprint or iris scan—unlike an alphanumeric password—cannot be

---

[56] Federal Communications Commission, *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice over Their Personal Information, https://apps.fcc.gov/edocs_public/attachmatch/DOC-341938A1.pdf.*

[57] *See* U.S. Patent Application No. 13/652,198, Publication No. 20130138506 (published May 30, 2013) (Google Inc., applicant) ("demographics data may include a user's age, gender, race, ethnicity, employment status, education level, income, mobility, familial status (*e.g.,* married, single and never married, single and divorced, etc.), household size, hobbies, interests, location, religion, political leanings, or any other characteristic describing a user or a user's beliefs or interests."); U.S. Patent Application No. 14/316,569, Publication No. 20140310268 (published Oct. 16, 2014) (Google Inc., applicant).

[58] *See* Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular,* Vox, Apr. 4, 2017, *https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll.*

[59] *See* Alex Byers, *House Votes to Revoke Broadband Privacy Rules,* Politico, Mar. 28, 2017, *https://www.politico.com/story/2017/03/house-votes-to-revoke-broadband-privacy-rules-236607.*

[60] Terrell McSweeny, Commissioner, Fed. Trade Comm'n, Remarks on *"The 3Future of Broadband Privacy and the Open Internet: Who Will Protect Consumers?"* (Apr. 17, 2014), at 4, *https://www.ftc.gov/system/files/documents/public_statements/1210663/mcsweeny_-_new_americas_open_technology_institute_4-17-17.pdf.*

[61] C.G.S.A. § 38a-999b(a)(2) ("health insurer, health care center or other entity licensed to do health insurance business in this state, pharmacy benefits manager . . . third-party administrator . . . that administers health benefits, and utilization review company.").

[62] West's Ann.Cal.Bus. & Prof.Code § 22584(d)(1) (schools must "[i]mplement and maintain reasonable security procedures and practices . . . and protect that information from unauthorized access, destruction, use, modification, or disclosure.").

[63] *https://ikeepsafe.org/last-years-education-data-privacy-legislation-trends/*

[64] M.S.A. § 325M.05 (must "take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information.").

[65] V.T.C.A., Bus. & C. § 521.052 ("implement and maintain reasonable procedures . . . to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.").

[66] States that have done this include Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming.

changed after it has been compromised. A large number of states also now require companies to notify consumers about breaches of medical or health data—information that can be used in aid of medical identity theft, potentially resulting in fraudulent healthcare charges and even introduction of false information into one's medical record.[67]

And states are doing other important work on privacy as well. In addition to the California Consumer Privacy Act,[68] California also has a law requiring notification about breaches of information collected through an automated license plate recognition system.[69] Vermont has the Data Broker Act.[70] And Illinois has the Biometric Information Protection Act.[71]

To avoid doing harm to consumers benefiting from these existing consumer protections, any Federal legislation on privacy or data security must preserve strong state standards.

4. Conclusion

I am grateful for the Committee's attention to these important issues, and for the opportunity to present this testimony. I look forward to your questions.

The CHAIRMAN. Thank you, Ms. Moy.

Ms. O'Connor.

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

Ms. O'CONNOR. Chairman Thune, Mr. Markey, and members of the Committee.

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology about the need for Federal privacy legislation.

CDT is a nonpartisan, nonprofit 501(c)(3) charitable organization founded in 1994, dedicated to advancing the rights of the individual in the digital world. We work on issues of individual privacy, freedom of expression, freedom from surveillance, and we are also seeking to advance innovation and preserving a global, open Internet.

My views today are informed not only by the research and advocacy of the lawyers, policy experts, and technologists at CDT, but by my own work on privacy and data issues across three decades. I have counseled Internet startups, served as a privacy leader in three companies, and was honored to have served as the Chief Privacy Officer for two Federal Government agencies under President George W. Bush.

I am also a technology enthusiast and an optimist. I believe in the power of Internet technology to improve our lives, as it has my own, as a consumer, as a member of my community, and as a busy working mother.

Today, my message is simple: privacy is about people. Privacy is about the digital and real world data breadcrumbs we leave behind, the things we say and do, the choices we make, the way we

---

[67] *See* Joshua Cohen, *Medical Identity Theft—The Crime that Can Kill You,* MLMIC Dateline (Spring 2015), available at *https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE_Spring15.pdf* ("A patient receiving medical care fraudulently can lead to the real patient receiving the wrong blood type, prescription, or even being misdiagnosed at a later time."). Medical or health data is covered by breach notification laws in Alabama, Arkansas, California, Delaware, Florida, Illinois, Kentucky, Maryland, Montana, Nevada, North Dakota, Oregon, Puerto Rico, Nevada, Rhode Island, Texas, Virginia, and Wyoming.

[68] California Consumer Privacy Act, *https://www.caprivacy.org/* (last visited October 7, 2018).

[69] West's Ann.Cal.Civ.Code § 1798.82(h)

[70] Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers,* TechCruch, May 27, 2018, *https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/*.

[71] 740 ILCS 14/1 *et seq.*

spend our time, and how the data about all of these things can affect what we see, and know, and achieve in the future.

Importantly, this is no longer only a question for tech sector companies. It is an issue for every company that uses data. You are online almost everywhere. You interact with and are observed by Internet-enabled devices as you walk down the street, as you browse in the aisles of your grocery store. Information is being collected in the dashboard of your car, in your kids' schools, and in your kitchen.

It is time to consider the impact of the ubiquitous data collection and to provide greater clarity and constraint on the collection and use of this information. Just as the United States has led the world on technology and data innovation, must we now engage in the leadership on the governance of these innovations.

It is time for baseline rules to provide certainty for all consumers and all companies, large and small, that recognize the rights of the individual in their own data and to rebalance the power differential in the data driven economy.

The Center for Democracy & Technology encourages you to pass baseline privacy legislation with at least the following elements:

First, a comprehensive baseline Federal privacy law should apply broadly to all personal data and all commercial entities whose data use is currently unregulated. Existing privacy protections should not be weakened and important gaps in coverage should be filled.

Second, the law should include individual rights like the ability to access, correct, delete, and move personal information. These values are already ensconced in both the California law and the GDPR. Certainly, these provisions should be carefully drafted to ensure that companies can engage in their basic business practices and secure their own systems. And the regulatory structures and the enforcement mechanisms must be tailored to our U.S. approach.

However, the law must recognize an individual's ongoing interest in his or her own data and assert the right of the individual to understand the consequential decisions made about them.

Third, Congress should prohibit the collection, use, and sharing of certain types of data when not necessary for the immediate provision of the service.

One way to do this is to declare it presumptively unfair under Section 5 of the FTC Act for companies to use highly sensitive data such as location information, microphone and camera information, children's information, health information, and biometrics for secondary purposes.

Fourth, the FTC should be expressly empowered to investigate data abuses that result in discriminatory advertising and other practices.

Finally, fifth, a Federal privacy law should be clear on its face and provide specific guidance to companies and markets about legitimate data practices. The law should ensure that the Federal Trade Commission is empowered to enforce and provided with sufficient resources and original fining authority.

Congress should explicitly empower the State attorneys general to enforce the law and any implementing rules.

Achieving meaningful baseline privacy legislation will be challenging, but it is essential to continuing American leadership on innovation, creating confidence and certainty for individuals and for institutions, and restoring lost consumer trust.

Your leadership is needed urgently. Thank you.

[The prepared statement of Ms. O'Connor follows:]

PREPARED STATEMENT OF NUALA O'CONNOR, PRESIDENT AND CEO, CENTER FOR DEMOCRACY & TECHNOLOGY

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to testify about the state of consumer privacy law, lessons learned from recent state law efforts, and opportunities for a Federal privacy law. CDT is a nonpartisan, nonprofit 501(c)(3) charitable organization dedicated to advancing the rights of the individual in the digital world. CDT was founded in 1994 by pioneering Internet advocates Jerry Berman, Janlori Goldman, Jonah Seiger, Deirdre Mulligan, and Danny Weitzner. CDT's founding coincides with the dawn of the commercial internet, and CDT continues to focus on the critical issues of protecting and elevating individual privacy, freedom of expression, and freedom from surveillance, while also seeking to advance innovation and preserve a global, open Internet. CDT has offices in Washington, D.C., and Brussels, and is funded by foundation grants for research and writing, corporate donations for general operating and program support, and individual program and event donations.[1]

I have been honored to serve CDT and the public interest for the past five years as President and CEO. My viewpoints today are not only informed by the research, analysis, and advocacy of the lawyers, policy analysts and technologists at the Center for Democracy & Technology, but also by almost 30 years of professional experience, much in the privacy and data realm. While in the private practice of law, I counseled some of the internet's earliest commercial websites; I have served as a corporate privacy leader at General Electric, Amazon, and DoubleClick; and was honored to have served as the chief privacy officer for two Federal government agencies—the U.S. Department of Commerce and the U.S. Department of Homeland Security. When I was appointed by President George W. Bush as the first chief privacy officer at the Department of Homeland Security under Secretary Tom Ridge, I was the first statutorily mandated CPO in the Federal service.

CDT submits this testimony and engages in this work informed by the underlying belief that internet-enabled technologies have the power to change lives for the better. And yet, nearly 25 years on from the dawn of the commercial internet, it is appropriate that we take stock of where we are, and where we are going. As with many new technological advancements and emerging business models, we have seen exuberance and abundance, and we have seen missteps and unintended consequences. International bodies and U.S. states have responded by enacting new laws, and it is time for the U.S. Federal government to pass omnibus Federal privacy legislation to protect individual digital rights and human dignity, and to provide certainty, stability, and clarity to consumers and companies in the digital world.

The Need for Federal Legislation

The U.S. privacy regime today does not efficiently or seamlessly protect and secure Americans' personal information. Instead of one comprehensive set of rules to protect data throughout the digital ecosystem, we have a patchwork of sectoral laws with varying protections depending on the type of data or the entity that processes the information. While this approach may have made sense decades ago, it now leaves a significant amount of our personal information—including some highly sensitive or intimate data and data inferences—unprotected.

Our current legal structure on personal data simply does not reflect the reality that the Internet and connected services and devices have been seamlessly integrated into every facet of our society. Our schools, workplaces, homes, automobiles, and personal devices regularly create and collect, and, increasingly, infer, intimate information about us. Everywhere we go, in the real world or online, we leave a trail of digital breadcrumbs that reveal who we know, what we believe, and how we behave. Overwhelmingly, this data falls in the gaps between regulated sectors.

[1] All donations over $1,000 are disclosed in our annual report and are available online at: *https://cdt.org/financials/*.

The lack of an overarching privacy law has resulted in the regular collection and use of data in ways that are unavoidable, have surprised users, and resulted in real-world harm. A constant stream of discoveries shows how this data can be repurposed for wholly unrelated uses or used in discriminatory ways:

- Madison Square Garden deployed facial recognition technology purportedly for security purposes, while vendors and team representatives said the system was most useful for customer engagement and marketing.[2]
- Application developer Alphonso created over 200 games, including ones targeted at children, that turn on a phone's microphone solely for marketing purposes.[3]
- Office Max mailed an advertisement to a Chicago man with "Daughter Killed In Car Crash" in the addressee line.[4]
- Facebook permitted housing advertisements to be obscured from parents, disabled people, and other groups protected by civil rights laws.[5]

The lack of an overarching privacy law has also resulted in absurd legal outcomes. Consider personal health information; whether this information is protected by Federal privacy law depends on who possesses it. Healthcare and health insurance providers are required to keep health information confidential under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), but no one else is, including health and fitness device and app developers that are regularly collecting some of the same information.[6] Americans' privacy interest in health information does not diminish because it is processed by an app developer instead of a healthcare provider.

While the Federal Trade Commission's ability to police unfair and deceptive practices provide a backstop, large gaps in policies around access, security, and privacy exist, which confuse both individual consumers and businesses. Because the FTC is prohibited from using traditional rulemaking processes, the agency has created a "common law" of privacy and security through its enforcement actions.[7] Creating proactive privacy rights through a process-of-elimination approach will not be able to keep up with advances in technology and the explosion of device and app manufacturers.

Without legislation, we may be stuck in a framework based on notice and consent for the foreseeable future.[8] "Notice" is provided through a presentation of legal terms and conditions, while "consent" is any action that signifies the acceptance of those terms. This model encourages companies to write permissive privacy policies and enticing users agree to data collection and use by checking (or not unchecking) a box. This model persists despite the fact that few individuals have the time to read privacy notices,[9] and it is difficult, if not impossible, to understand what they say even if they are read.[10]

Even if an individual wants to make informed decisions about the collection, use, and sharing of their data, user interfaces can be designed to tip the scales in favor of disclosing more personal information. For example, the FTC reached a settlement with PayPal in February after its Venmo service misled users about the extent to

---

[2] Kevin Draper, Madison Square Garden Has Used Face-Scanning Technology on Customers, NYT, Mar. 13, 2018.

[3] Sapna Maheshwari, That Game on Your Phone May Be Tracking What You Watch on TV, NYT, Dec. 28, 2017, *https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html.*

[4] Nestia Kwan, OfficeMax Sends Letter to "Daughter Killed In Car Crash," nbcchicago.com, Jan 14, 2017, *https://www.nbcchicago.com/news/local/OfficeMax-Sends-Letter-to-Daughter-Killed-in-Car-Crash-240941291.html.*

[5] Brakkton Booker, HUD Hits Facebook for Allowing Housing Discrimination, NPR, Aug. 19, 2018, *https://www.npr.org/2018/08/19/640002304/hud-hits-facebook-for-allowing-housing-discriminati on.*

[6] HHS, Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA 6, *https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.* This is an imminent concern, as the Centers for Medicare and Medicaid Services are advancing the Blue Button 2.0 Standard, which would make more healthcare information available to developers.

[7] Daniel Solove and Woody Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia L. Rev. 583, (2014).

[8] See, *e.g.,* Fred Cate, The Failure of Fair Information Practice Principles, in THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES 342, 351 (Jane Winn ed., 2006); and Solon Barocas & Helen Nissenbaum, On Notice: The Trouble with Notice and Consent, Proceedings of the Engaging Data Forum, (2009).

[9] Aleecia McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: A Journal of Law and Policy 543, (2008).

[10] Joel Reidenberg, Presentation, Putting Disclosures to the Test (2016), available at *https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.*

which they could control the privacy of their financial transactions.[11] Users' transactions could be displayed on Venmo's public feed even if users set their default audience to private. In the case of the Cambridge Analytica disclosure, users purportedly consented to disclosing information by filling out a quiz, but had no way of foreseeing how that information would be used.[12]

Beyond any one privacy decision, the sheer number of privacy policies, notices, and settings or opt-outs one would have to navigate strain individuals' cognitive and temporal limitations. It is one thing to ask an individual to manage the privacy settings on their mobile phone; it is another to tell them they must do the same management for each application, social network, and connected device they use. Dozens of different data brokers operate different opt-outs.[13] Further, people operate under woefully incorrect assumptions about how their privacy is protected.[14] Privacy self-management alone is neither scalable or practical for the individual. Burdening the individual consumer or citizen with more and more minute choice and decision-making, absent some reasonable boundaries, will not provide the systemic changes we need.[15]

It is important to note that privacy harms can still emerge separate and distinct from any single individual's choice or consent and despite an individual's attempts to exercise a choice. A service's data practices can harm individuals who are not even users of the service. This spring, for example, the fitness tracking app Strava displayed a heatmap of users' runs that revealed the locations and outlines of military and covert activity that could be used to identify interesting individuals, and track them to other sensitive or secretive locations.[16] The harms stemming from this type of disclosure can reach people who never used the app and thus never had the option to "consent" to Strava's data policies.

CDT is not the only entity to critique notice and consent as the predominant privacy control in U.S. law. Just last month, the National Telecommunications and Information Administration (NTIA) acknowledged the shortcomings of the notice-and-consent model. The administration's request for comment on privacy noted that "relying on user intervention may be insufficient to manage privacy risks."[17] Of course, constructing a new framework is complicated and will only happen by way of statute. It is time to rebuild that trust by providing a baseline of protection for Americans' personal information that is uniform across sectors, that follows the data as it changes hands, and that places clear limits on the collection and use of personal information.

What Legislation Should Include

Instead of relying primarily on privacy policies and other transparency mechanisms, Congress should create an explicit and targeted baseline level of privacy protection for individuals. As discussed below, legislation should enshrine basic individual rights with respect to personal information; prohibit unfair data processing; deter discriminatory activity and give meaningful authority to the FTC and state attorneys general to enforce the law.[18]

Individual Rights in Data

A Federal law must include basic rights for individuals to access, and in some instances, correct their personal data held by companies; individuals should also have

---

[11] Press release, FTC, Feb. 28, 2018, *https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.*

[12] Kevin Granville, Facebook and Cambridge Analytica: What you Need to Know as Fallout Widens, NYT, Mar. 19, 2018, *https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.*

[13] Yael Grauer, Here's a Long List of Data Broker Sites and How to Opt-Out of Them, Motherboard (Mar. 27, 2018), *https://motherboard.vice.com/en_us/article/ne9b3z/how-to-get-off-data-broker-and-people-search-sites-pipl-spokeo.*

[14] Joseph Turow, Let's Retire the Phrase 'Privacy Policy', N.Y. Times (Aug. 20, 2018), *https://www.nytimes.com/2018/08/20/opinion/20Turow.html.*

[15] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).

[16] Jeremy Hsu, The Strava Heatmap and the End of Secrets, Wired, Jan. 29, 2018, *https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.*

[17] National Telecommunications and Information Administration, Request for Comments on Developing the Administration's Approach to Consumer Privacy, Sept. 25, 2018, *https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.*

[18] While we do not address transparency per se in this statement, we assume that any legislation will include such provisions and are available to discuss possibilities in detail with Congressional offices.

the ability to easily delete or move information out of services.[19] It should also enshrine the right to know how and with whom personal data is shared. These overarching rights are relatively noncontroversial. Companies must already extend them to their EU users under the General Data Protection Regulation (GDPR), and elements of these rights are also at the core of the recent California Consumer Privacy Act. They have been recognized by the U.S. government and international bodies for decades, albeit in voluntary form.[20] With appropriate, tailored exceptions, these provisions can be crafted in a way that does not unduly burden companies' business practices or interfere with the provision of services.

Where feasible, these rights should apply not only to data that users have shared with a company but also to information that a company has observed or inferred about users, such as their location, web browsing information, and advertising categories they have been placed in. Inferences can be more sensitive and relevant than the data a user directly discloses to a company, are often invisible to the user, and can be the basis for decisions that have significant effects on people's lives. A 2013 report by this committee found that data brokers created and sold consumer profiles identifying people as "Rural and Barely Making It," "Ethnic Second-City Strugglers," and "Retiring on Empty: Singles." This information can be used to target vulnerable consumers with potentially harmful offers, such as payday loans.

Federal legislation should enshrine rights like access, deletion, and portability, but it cannot stop there. While these rights give individuals control over their data in some sense, they are not a substitute for the systemic changes we need to see in data collection and use.

Declaration that certain data practices are presumptively unfair

Users are often comfortable providing the data required to make a service work, but in providing that information, they are often asked to consent to long, vague lists of other ways in which that data may be used or shared in the future. These future uses are often couched in terms such as research, improving services, or making relevant recommendations, and the precise nature of these secondary uses are often difficult for users to foresee.

While data provided in the context of a commercial transaction can often be considered part of an ongoing business relationship, and used in the context of future transactions between the parties, there are some types of data and some processing practices that are so sensitive that they should be permitted only to provide a user the service they requested, and prohibited from entering the opaque and unaccountable market of secondary uses. These practices could include the collection and processing of precise location information, the use of biometric information to identify individuals, and the use of healthcare information or children's information for targeted marketing. For example, if a user opts-in to a feature that allows her to unlock her phone with her face, her unique face data should be used only to provide that feature, and perhaps improve performance of that feature. But the data should not be used, for example, to unexpectedly recognize and tag her in photos or for other secondary purposes—without her specific, separate choice to engage in that service. Repurposing these types of data for a purpose far afield from the primary transaction without independent indication of consent should generally be considered an unfair practice under Section 5 of the FTC Act.

Rules to prevent discriminatory effects

Independent entities have attempted to study whether online advertising can facilitate the violation of long-standing civil rights laws.[21] These studies have determined that in some cases, advertisers are able to prevent parents, the disabled, and other protected classes from receiving advertisements for housing or employment. This has prompted some platforms to reevaluate and reform their systems.[22] Because online advertising is ephemeral, individuals and government agencies may face unique challenges in defending civil rights. To that end, a data privacy statute should focus on the potential for opaque discriminatory effects based on data decisioning, and should articulate a non-discrimination standard. The FTC should

---

[19] *https://eu.usatoday.com/story/tech/columnist/2017/11/12/web-companies-should-make-easier-make-your-data-portable-ftcs-mcsweeny/856814001/*

[20] Robert Gellman, Fair Information Practices: A History, 2012, *https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.*

[21] See Booker, note 5; Julia Angwin, et. al, Dozens of Companies are Using Facebook to Exclude Older Workers From Jobs, Dec. 20, 2017, *https://www.propublica.org/article/facebook-ads-age-discrimination-targeting.*

[22] Facebook Agrees to Prevent Discriminatory Advertising, LAT, July 24, 2018, at *http://www.latimes.com/business/technology/la-fi-tn-facebook-discrimination-advertising-20180724-story.html;*

be directed to write rules to mitigate the ways new advertising models disproportionately disadvantage protected classes.

Meaningful enforcement mechanisms

Affirmative individual rights and data collection and use restrictions may ultimately be meaningless absent strong enforcement. While we believe that the Federal Trade Commission has been effective as the country's "top privacy cop," it is also an agency that desperately needs more resources. Funding for the agency has fallen five percent since 2010, and its resources are strained.[23] In 2015, the FTC had only 57 full time staff working in the Department of Privacy and Identity Protection, with additional staff working in enforcement and other areas that could touch on privacy.[24] In additional to more FTC funding, Federal legislation must include two new statutory enforcement mechanisms.

First, the FTC must be given the ability to extract meaningful fines from companies that violate individuals' privacy. Because much of the Commission's existing privacy enforcement falls under Section 5 of the FTC Act, it does not possess original fining authority and companies are functionally afforded one free "bite at the apple" regardless of the intent or impact of a privacy practice.[25] At present, before a company may be fined for violating individuals' privacy, it must first agree to and be placed under a consent decree, and then subsequently violate that agreement.

Relying solely on consent decree enforcement has been inadequate to protect user privacy. The penalties for violating a decree may be so insignificant that they do not have the intended deterrent effect. For instance, when Google agreed to pay a $22.5 million penalty for violating the 34 terms of its consent order in 2012, this was approximately five hours worth of Google's revenue at the time.[26] Additionally, Facebook has been under a consent decree throughout the entire duration of its dealing with Cambridge Analytica, as well as its merger of data between its Facebook platform and WhatsApp.[27]

Second, state attorneys general must be granted the authority to enforce the Federal law on behalf of their citizens. State attorneys general have been enforcing their own state consumer privacy laws for decades, first under state unfair and deceptive practice laws and more recently under state statutes targeted at specific sectors or types of data.[28] Employing their expertise will be necessary for a new Federal privacy law to work. A law with the scope we are proposing will bring large numbers of previously unregulated entities into a proactive regime of new privacy and security requirements. There will simply be no way for a single agency like the FTC to absorb this magnitude of new responsibilities.

Additionally, each state has a unique combination of demographics, prevailing industries, and even privacy values, and many privacy or security failures will not affect them equally. State attorneys general must be able to defend their constituents' interest even if the privacy or security practice does not rise to the level of a national enforcement priority. Arguably, local enforcement is best for small businesses. A state attorney general's proximity to a small business will provide context that will help scope enforcement in a way that is reasonable.

Conclusion

The existing patchwork of privacy laws in the United States has not served Americans well, and as connected technologies become even more ubiquitous, our disjointed privacy approach will only lead to more unintended consequences and harms. We risk further ceding our leadership role on data-driven innovation if we do not act to pass baseline privacy legislation. Effective privacy legislation will shift the balance of power and autonomy back to individual consumers, while providing

---

[23] David McCabe, Mergers are spiking, but antitrust cop funding isn't, AXIOS, May 7, 2018, *https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486–4a08-ab57-d3535ae43b52.html;* see also *https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/?utm_term=.c6c304221989*

[24] *https://www.ftc.gov/system/files/documents/reports/fy-2016-congressional-budget-justification/2016-cbj.pdf*

[25] Dissenting Statement of Commissioner J. Thomas Rosch, In the Matter of Google Inc., FTC Docket No. C–4336 (Aug. 9, 2012), *https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googleroschstatement.pdf.*

[26] *Id.* Commissioner Rosch noted that a $22.5 million fine "represents a de minimis amount of Google's profit or revenues."

[27] Laura Sydell, FTC Confirms It's Investigating Facebook for Possible Privacy Violations, NPR (March 26, 2018), *https://www.npr.org/sections/thetwo-way/2018/03/26/597135373/ftc-confirms-its-investigating-facebook-for-possible-privacy-violations.*

[28] Danielle Keats Citron, The Privacy Policy Making of State Attorneys General, 92 Notre Dame L. Rev. 747 (2016), *https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4693&context=ndlr.*

a more certain and stable regulatory landscape that can accelerate innovation in the future. The time is now to restore the digital dignity for all Americans. Congress must show their leadership and pass a comprehensive privacy law for this country.

The CHAIRMAN. Thank you, Ms. O'Connor.

We will go right into the questions.

Dr. Jelinek, as you know, Facebook is now being investigated by Ireland's Data Protection Authority in response to the recent cyber attack affecting 90 million users. I think this is an interesting case study that will help our members better understand how the GDPR is likely to be enforced.

Could you explain exactly what your role will be as the head of GDPR enforcement?

Dr. JELINEK. I just want to explain, if you will allow me, the functioning of the one stop shop mechanism according to the GDPR. How does this work in practice?

When a cross-border case is issued, or a cross-border data breach is issued, like it is with the Facebook issue, we will look into the system that is going to be the lead supervisory authority. In this case, for sure, this is Ireland.

The Irish DPC is going to put this in their internal system because we share a common IT system. Irish DPC is asking the other Data Protection Authorities if they think they are concerned. They are concerned if consumers or people in their countries are offended. In most of these cases, in this it will be that all the other Data Protection Authorities are concerned authorities. That is the first step.

The second step is the Irish DPC is investigating the case, is the interlocutor for Facebook, and then is making a draft decision on this data breach, and shares these draft decisions with the other concerned authorities.

If the other concerned authorities have any objections, and the Irish DPC does not take this into account for their draft, it will trigger the Board. This issue is coming to the Board that is working as an arbitration mechanism.

If they cannot come to a common decision, then the Board decides whether these objections, the Irish DPC has to take into account or not with a two-third majority, and the Irish DPC has to follow this decision of the Board.

That means the Board is only then enabled to act when the DPA's are not inline together, if they are not of the same opinion regarding their decision on a case, then we are going to act.

The CHAIRMAN. To the best of your knowledge, how many GDPR investigations have been opened so far across the E.U.?

Dr. JELINEK. So far, at this moment, the figures are from the first of October, we have 272 cases regarding identifying who is going to be the lead supervisory authority and who is going to be the concerned supervisory authority.

Just to give an example, most of the cases, the Irish or the Luxembourg DPA, are the lead supervisory authority. All supervisory authority is in five cases, lead supervisory authority.

There are 243 issues regarding mutual assistance according to Article 61 of the GDPR, and there are already made 23 opinions regarding data protection impact assessment.

So you see, beginning with May 25, the Board is already working on quite many cases.

The CHAIRMAN. It is a busy docket.

Dr. JELINEK. Yes.

The CHAIRMAN. So from your perspective, what company practices have generated the most complaints or concerns from consumers?

Dr. JELINEK. I think the complaints that are the most at the moment are complaints regarding consent.

The CHAIRMAN. All right.

Mr. Mactaggart, businesses have raised concerns that the CCPA will interfere with, or even prohibit, certain practices that consumers like. For example, some retailers have suggested that the law will make it impossible for them to have customer loyalty programs that reward their best customers.

Do you think these are fair concerns?

Mr. MACTAGGART. Senator, this is one that we have heard before and frankly, it just mystifies us. We cannot see anything in the law that prohibits loyalty cards.

And, in fact, we think that there is nothing in the law that prohibits companies to have a first party relationship with consumers for using their data if the consumer consents. So we cannot see that. I am happy to respond to any of your staff members in the QFRs after.

The CHAIRMAN. OK. If that is the case, the question of whether or how you would address them in Federal legislation, and maintain the same level of consumer privacy protection, it seems like that would be an area of discussion.

Obviously, you say that it is not an issue, but that is an argument that is being made by those that are in that industry.

Mr. MACTAGGART. I think one of the concerns, and Senator Markey brought it up, is with respect to whether you are able to offer different pricing mechanisms to consumers who want to put a premium on privacy or not. It is a thorny issue.

What we ended up saying is that the companies were not able to, but we limited it and we said that the choice cannot be coercive. I mean, the companies increase price for privacy. It cannot be coercive. It cannot be usurious. It cannot be unjust or unreasonable.

I think we always tried to strike a balance to allow companies to have a different arrangement with consumers who want privacy. And this is, I will say, this is an area of contention because some people feel very strongly that there should be absolutely no differentiation.

What we feel is that if we let the market decide alone, but we have some certain basic limitations, that that is a way of allowing the companies flexibility because you do not want to be in a situation where you are saying that a company has to offer a product for free.

The CHAIRMAN. Are there any provisions of the CCPA that you think could benefit from further revision or clarification? I know there are some discussions out there about doing that before it becomes enacted.

Mr. MACTAGGART. Sure, Senator. We just spent a couple of years doing this and the opponents will say it was quickly done and

badly drafted. But essentially the rushed part was the actual passing of the legislation in the final couple of weeks and that was rushed. But essentially the language was taken from the initiative. So we feel it works very well as-is.

We gave up some things; that was just part of the compromise. There was a whistleblower provision in there and I do feel that would have been nice to have because sometimes it is so hard to understand what is going on in these very complicated companies that I think that would have been a useful thing to have.

But importantly, one of the things that we did was we gave the California Attorney General the right to issue regulations. I think that is so important going forward if you do a Federal bill to give the rulemaking authority to the enforcing authority because you do not want a bill that is going to be stuck in time.

And so, we feel that because we gave the AG the right to issue regulations that will allow the bill to be flexible with time.

The CHAIRMAN. Thank you.

Senator Markey.

Senator MARKEY. Thank you, Mr. Chairman.

Ms. Moy, should companies be able to tell consumers that if they do not agree to share nonessential data, they cannot receive the service or the product?

Ms. MOY. No, no. They should not be able to tell consumers that.

And I think that that really gets back to the idea, to the question of what constitutes choice, in a notice in choice. Even if we have no notice in choice, which is, as I have said before, I think not enough. I think we still need use restrictions as well.

But a choice has to be a real choice. I think that this is something that the GDPR does well. It says the consent must be freely given. When a company says, "Accept our practices with your data or do not use the service," that is not a free choice.

Senator MARKEY. OK, great.

Now, should companies be allowed to offer financial incentives in exchange for Americans' personal information?

Ms. MOY. I support skepticism toward financial incentives for certain data practices because I do recognize that while there may be a value that consumers enjoy in exchange for their data, as Mr. Mactaggart just mentioned, oftentimes the financial incentives that companies offer, or the financial penalties that they levy against consumers who decline to give consent, are not truly commensurate with the value of the information as the company realizes that they are, in fact, coercive.

Senator MARKEY. Should companies only be permitted to collect the information that is essential to providing the service or product in question? Should a flashlight application be able to collect information about my interests and location?

Ms. MOY. Yes, right. I agree with you. Information collected by a site or service should only be that information that is necessary to actually provide the site or service. That seems like a bare minimum.

Senator MARKEY. So Ms. Moy, AT&T recently announced that it will stop sharing user's location information with data brokers. Facebook has stated that it will stop allowing advertisers to use in-

formation about users' race and religion to exclude some users from seeing particular advertisements.

Do you agree that such practices should be banned, not just left to voluntary compliance by companies? Should a Federal privacy bill establish limits on how companies can use Americans' information; not rely upon voluntary actions taken by individual companies?

Ms. MOY. A Federal privacy bill absolutely should establish limits. The case that you mentioned with major phone carriers providing location information about their consumers to third parties who had paid for it is a completely egregious use of consumer information.

Senator MARKEY. Great. Should consumers have the right to access, correct, and delete their personal information in matters inconsistent with existing laws?

Ms. MOY. Yes.

Senator MARKEY. Should Congress establish enhanced data security standards to protect consumers' private information?

Ms. MOY. Absolutely. It is sorely needed.

Senator MARKEY. Let me move onto children's privacy. I would like to go to you, Mr. Mactaggart. It is a subject that Senator Blumenthal and I have been working on.

In 2018, we are seeing issue after issue where children's privacy is being compromised. I am the author of the 1998 Children's Online Privacy and Protection Act, COPPA, which was a law I wrote back in 1998 with Congressman Billy Tauzin.

Mr. Mactaggart, the California law requires both online and offline companies, regardless of whether these businesses target children, to obtain opt-in consent from parents of children under 13 before collecting and selling their personal data. In addition, companies will be required to obtain affirmative consent from consumers between the ages of 13 and 16 in order to sell their data.

Mr. Mactaggart, do you believe a Federal law should also grant special protections for 13, 14, and 15 year olds?

Mr. MACTAGGART. Yes, Senator.

Senator MARKEY. Do you agree with that, Ms. Moy?

Ms. MOY. Yes.

Senator MARKEY. In terms of the eraser button which, at least, should be usable by parents with children 15 and under, do you agree that there should be an eraser button, which is part of the law? So that if a 12, 13, 14, or 15 year old has done something online which is inappropriate, that it does not haunt them for the rest of their life? That they should be able to just demand through the parent that that information is erased?

Do you agree with that, Mr. Mactaggart?

Mr. MACTAGGART. Yes, Senator, and all I would say is that the First Amendment does have implications here. And so, when we looked into it, it gets a little difficult, but yes, I do.

Senator MARKEY. Yes. Ms. Moy.

Ms. MOY. Yes, as the mother of a 5-year old, I am terrified about the things that I know he will surely post online when he is 13. I do support a right to deletion of some sort for teenagers.

Senator MARKEY. Can we square that with the First Amendment, Ms. Moy?

Ms. MOY. I think that there are ways to do it, yes.

Senator MARKEY. Great. Do you agree with that Mr. Mactaggart?

Mr. MACTAGGART. Absolutely, yes. I just think it is thornier than it looks.

Senator MARKEY. OK, great. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey.

Senator Wicker.

STATEMENT OF HON. ROGER WICKER,
U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Dr. Jelinek, under E.U. policy, your Board could have chosen the regulation route or the directive route. A regulation places a binding legal force throughout the continent. A directive would simply have had each country try to implement according to their own national laws.

GDPR went the regulation route. The goal was and is to have one set of privacy rules that are interpreted in a uniform way throughout the continent.

Why did you do that, and why was it important to have one data privacy policy instead of each member country having their own?

Dr. JELINEK. Thanks, Senator, for this question.

The E.U. already had a Data Protection Directive from 1995 on, and this Data Protection Directive had to be set into the national laws of the 28 member states. So there were five laws, even if they had the same fundament.

During the last 20 years, the E.U. considered that it would be much better to have one applicable law according for the whole continent, for the whole E.U. And so, it started in 2012 to negotiate the regulation, and the regulation was finalized in 2016, and entered into force and entered into application on the twenty-fifth of May 2018 to have one continent, one law.

Senator WICKER. OK. With regard to how it is being implemented and how people have reacted to this, there have been reports that upon implementation, several companies shutdown their operations, blocked access to European users, or required European consumers to pay for access to online content.

Could you comment about that? Has that been overblown or am I accurate in what I have stated there? Why would the companies have done so?

Dr. JELINEK. I cannot contribute to why the companies have done that.

But as far as I can tell you is most of the companies on either side of the ocean, U.S. companies and European companies, were preparing quite well for the entering into application of the GDPR. They had more than two years' time to prepare and the twenty-fifth of May was not the end of preparation. It was just the beginning of the common journey in the new field of data protection.

Data protection was not that new because, as I just mentioned, we already had a directive from 1995 on and the GDPR was no revolution but just an evolution of the law that already existed.

Senator WICKER. OK. Let me ask Ms. O'Connor about this preemption idea.

Ms. Moy suggested in her testimony that what we do here in Congress should establish a floor, not a ceiling. It seems to me that you feel the other way.

Is it your position that there should be one privacy standard for the entire country coming out of this Congress; and if so, why?

Ms. O'CONNOR. I think it is better for American consumers to know what the rules are no matter what company they are dealing with or what state that company is based in. However, I am not seeking a lower standard than we have. We would not seek weakening of existing laws. We would very much applaud the effort that was made in California and want to see strong protections.

So while I think it is too early to talk about preemption, I think one of your colleagues has suggested that the price of preemption would be very, very high.

Senator WICKER. OK. Why would a patchwork negatively affect consumers, though? You alluded to that just now in your verbal answer, and it is in your written testimony too.

How would it affect consumers adversely to deal with a patchwork from state to state?

Ms. O'CONNOR. I think there would be uncertainty and a lack of clarity about what the rules and guidelines are for each individual dealing with companies all over the country. And also, it does not get us standing in the global dialogue on data protection. Europe is leading the way, and other countries and regions are following the European model.

I would like to see the United States offer an alternative that has strong baseline protections. I would agree with Ms. Moy that it is a floor, not a ceiling, but that would provide some leadership from Congress for all of the States' Attorneys General and the FTC to enforce.

Senator WICKER. Maybe you could supply on the record an example or two of how a consumer could be disadvantaged by a patchwork? We will just ask you to do that on the record. Will do you that?

Ms. O'CONNOR. I will do.

Senator WICKER. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Wicker.

Senator Blumenthal.

STATEMENT OF HON. RICHARD BLUMENTHAL, U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thanks, Mr. Chairman.

I want to thank you and our Ranking Member for pursuing this issue on a very bipartisan basis. I am working with a number of my colleagues from both sides of the aisle on a bill that, I hope, will have strong bipartisan backing that, in fact, sets a floor not a ceiling.

We can no longer rely on notice and choice, on voluntary standards, on transparency, and consent. There needs to be privacy by design. Call it a privacy bill of rights. Call it a mandatory standard or a floor. That kind of bill of rights should incorporate essential principles that both the European law and the California law embody.

I want to thank all of you for being here today, but particularly Mr. Mactaggart for championing this cause against great odds and strong adversaries in California as you did, and your continued dedication to this cause.

I want to ask all of you the same question I put to the executives of major companies that came before us.

Is there anybody here who believes that American citizens deserve less privacy protection than European citizens?

[No response.]

Senator BLUMENTHAL. Your answer is the same. Everybody agrees that Americans should have that same privacy.

Is there anybody here who believes that the people of Connecticut or anywhere else in the Nation should have less privacy protection than the people of California?

[No response.]

Senator BLUMENTHAL. No one. We all agree on that basic principle. I think this cause is one whose time has come.

I want to mention the elephant in the room. We learned last Monday of yet another breach of the public's trust by a big tech firm last May. Google discovered a vulnerability in its social network product, Google+, that left private data exposed to outside developers, more than 400 of them.

According to *The Wall Street Journal,* Google decided that it would not disclose the issue. In fact, it hid the problem to avoid bad press. Thanks to *The Wall Street Journal* for disclosing a memo—I believe it was *The Wall Street Journal*—from one policy staff member, who argued that disclosure would result in Google, quote, "Coming into the spotlight alongside, or even instead of, Facebook despite having stayed under the radar throughout the Cambridge Analytica scandal."

The fact is that consumers have no meaningful Federal protection for consumer data. All we have is congressional oversight right now, whistleblowers who come forth, and press reports.

Until there is an effective enforcer at the Federal or State level with Federal standards backed by strong resources and authority, consumers will continue to be at risk.

I will be calling later today in a letter to the FTC for an investigation of Google in connection with this incident. I hope to be joined by a number of my colleagues. I hope that European authorities will investigate.

Dr. Jelinek, do you have an interest as an investigator in this violation of basic norms by Google in the failure to disclose for months and months? Put aside the breach of standards and vulnerability that was discovered, the failure to disclose purposefully because of the potential embarrassment.

Dr. JELINEK. I just want to answer just briefly. The Irish DPC is already investigating the case and the Hamburg Data Protection Authority too because not each and every data protection authority is able to investigate because the breach was before the twenty-fifth of May.

This shows as a good example how easy it could be for consumers and for companies if they already had it. If the breach would have been after the twenty-fifth of May and Google would have made es-

tablishment in Europe, then they just would have had to face one investigator, one investigation.

So they will have to face more than one from the European authorities.

Senator BLUMENTHAL. My time is expired, but I am really delighted to hear that there will be an investigation. I hope it will be a combined and coordinated one with our Federal Trade Commission or other authorities in this country because I think this kind of deliberate concealment is absolutely intolerable.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal.

Senator Moran.

STATEMENT OF HON. JERRY MORAN,
U.S. SENATOR FROM KANSAS

Senator MORAN. Mr. Chairman, thank you.

Thank you to you and Senator Markey, and thank you for our witnesses for your presence here today.

I chair the Subcommittee of this Full Committee on Consumer Protection and Data Security. Our Subcommittee, as well as this Full Committee, remain totally committed to a better system than what we have today.

Let me begin with what, I hope, is a yes or no answer, what I think can be a yes or no answer, to Dr. Jelinek and Mr. Mactaggart.

I mentioned this in our hearing that we had on September 26, the privacy of consumer data. I support privacy rules that afford consumers the same protections no matter where they are in the Internet ecosystem. It appears to me that both GDPR and CCPA take a similar approach.

Rather than regulating the type of business handling the data, would you agree that regulating and enforcing privacy rules based on the sensitivity of the data collected, used, and transferred, or stored is the preferred approach and in the best interest of consumers in terms of certainty and transparency? I think that can be a yes or no answer.

Dr. Jelinek.

Dr. JELINEK. I think it is very important that the consumer knows which data is collected, which are they, and where are they stored, and how long they are stored. I think it is really important, yes, to know for the consumers.

Mr. MACTAGGART. Senator, we treat all personal information the same. So, yes.

Senator MORAN. That is the point, Dr. Jelinek, which I am trying to get to. It does not matter what ecosystem in the Internet world you are in. It does not matter who the provider is, we want people to be treated the same.

Dr. JELINEK. Yes, people have to be treated the same.

Senator MORAN. Thank you very much.

Mr. Mactaggart, the CCPA defines personal information to mean information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked directly or indirectly to a consumer or household.

Are you concerned that that broad definition of personal information sweeps in information that is not sensitive? What does it mean that information can be linked indirectly with a consumer or household? That sounds somewhat removed from information that can identify an individual.

Mr. MACTAGGART. Senator, we took that definition from preexisting California law.

I think one of the things to think about is that the game now is to find out what your device is. And so, we are trying to make sure that your device is captured in there.

Google was in here two weeks ago and they said they did not sell personal information. And then when pressed, they said, well, personal information is your name or your e-mail address. But the reality is, it is your device. If I know everything about your device, I know everything about you.

And so, we think our definition is appropriate becau8se it is linking back to an individual and it is being able to track them across whatever they do.

Senator MORAN. If I understand correctly, what I described as "broad," is intentional to alleviate others having a narrow definition.

Mr. MACTAGGART. Right. We are trying to avoid game playing. Again, go back to the fact that we gave the AG regulatory authority to issue regulations around this to clarify things if it does turn out to be a problem.

But also, technology is going to move and you want to be able to keep pace with the times.

Senator MORAN. Thank you very much.

Dr. Jelinek, Mr. Mactaggart's testimony described the differences between CCPA and GDPR. One of the specific points he made was that GDPR's requirements of obtaining consumer approval before collecting and processing their data would specifically harm new entrants to the marketplace since consumers are far less likely to provide upfront consent to newer, lesser known companies.

Do you think that Mr. Mactaggart's criticism of GDPR is valid?

Dr. JELINEK. I think it was not a criticism in that case. It is a different approach because I think it is important that you know if somebody is collecting your data and that you can give the consent for the processing.

Senator MORAN. This may be a follow up to you or maybe you, Mr. Mactaggart.

It is obvious, at least to me, that larger companies like those we had in front of us recently, they have large legal departments, compliance officers that allow them to better react or respond to the regulations proposed by either California or the European community, but smaller and newer companies are not likely to have those resources.

Do you have any concerns regarding this impact that the enforcement actions related to GDPR compliance could have on small entrepreneurial businesses?

Either one of you.

Dr. JELINEK. As the enforcement action, as the fines are only the last step, I think it is no problem because we can make warnings

and recriminations as the first two, not only fines. That is the first thing.

And the second thing, the second issue is the fines have to be proportionate, always proportionate. It always also proportionate if it is a big or a small company, and how they tried to comply before. It is not that it is possible to fine a small company as a big company because a small company has different revenue, has a different approach.

Senator MORAN. So what you are suggesting is that the ability to warn as compared to enforce, or if enforcement, the smaller the fine, that offsets the small nature of a business?

Dr. JELINEK. No, it is not to be dependent of the small or big business. It depends on the nature of the business because all the small businesses, if they are doing health apps, they have two people, but they are doing it in health apps.

This can be a business that is doing and just dealing with data, and so it is not a question if a business is big or small if there can be imposed fines.

It is a question of the nature of the business and the nature of the infringements. Article 83 of the GDPR shows us 11 grounds how to impose the fines.

Senator MORAN. Thank you very much.

Well, I have had a chance only to visit with two of you. I appreciate all of you being here.

The CHAIRMAN. Thank you, Senator Moran.

Senator Hassan.

STATEMENT OF HON. MAGGIE HASSAN,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator HASSAN. Thank you, Mr. Chair. Again, I want to thank you and Senator Markey for holding this hearing.

To all of the witnesses, thank you for being here today.

Dr. Jelinek, I wanted to start with a question to you. Under the GDPR, companies must notify consumers of a data breach on a, "occurrence standard." Several of the privacy principles that have been released by the industry call for a "harm standard," meaning the consumers would only be notified if a breach results in so-called "measurable harm."

And as Senator Blumenthal just referred to, earlier this week it was reported that Google experienced a multiyear data leak that affected over, approximately, 500,000 accounts. However, the information that was leaked did not reach any legal threshold that would require public disclosure of the leak.

This incident further highlights the need for a closer look at how we might structure data breach notification in Federal legislation as it is sorely concerning to me that an incident affecting this many people did not have to be disclosed publicly.

With this in mind, could you discuss why the craftors of the GDPR chose an "occurrence standard" over a "harm standard"?

Dr. JELINEK. As I was not negotiating the GDPR, I cannot tell you the reasons behind it.

Senator HASSAN. Yes.

Dr. JELINEK. But as far as we know, as regulators, the reason behind it is the timeline; 72 hours is quite enough to make a first

notice. That is the first thing because you have to look into the breach more thoroughly. It is clear that it cannot happen within the first 72 hours. That is the first thing.

The second thing, the measurable harm for the people, I think, first of all there are guidelines issued by the Working Party 29, endorsed by the EDPP at its first session, what is a measurable harm?

Senator HASSAN. Yes.

Dr. JELINEK. I am sure all of you in this room know what a measurable harm is because if you are already thinking as a company, "How could this affect my consumers?" you should notice them. As far as I know, there was no problem for all the big tech companies to make notice to their consumers, to reach out to them.

Senator HASSAN. Well, thank you. I appreciate that.

I wanted to follow up with another question to you. We talked a lot about how to prevent data breaches, but I do not think there has been enough discussion about how to limit the damage when a data breach actually occurs.

One of the best ways to do this is to limit what types of data a company can hold onto for an extended period of time.

For example, when I was Governor of New Hampshire, I worked with both law enforcement and privacy advocates in my state on automatic license plate reading technology. Under the compromise we worked out, law enforcement has access to license plate data for a brief period of time, but then the data is erased if the vehicle is not linked to a warrant or to an alert.

To me, that seems like the right kind of balance between utility and privacy, although I will bet right now that my law enforcement folks would argue that we still have not gotten that balance exactly right.

What are the reasons a company would need to store data for longer? How do we balance holding data for the possibility of using it for purposes such as innovation with the possibility that holding onto data could mean that more consumer information would unnecessarily be released in the event of a breach?

I will start with you, Dr. Jelinek, and then I will ask the others to weigh in.

Dr. JELINEK. Regarding to the GDPR, if you store the data longer than you need it, you do not act in accordance with the law. That is the first thing.

And the second thing is you just have to hold the data for the issue you are processing it. And so the best limitation is if you do not hold it longer, so you will not risk a breach.

Senator HASSAN. Yes, understood.

Would anybody else like to comment on that, Mr. Mactaggart or Ms. Moy?

Ms. MOY. Yes, the point that you raise about data retention is a really interesting one because the financial incentives are set up to encourage companies, in fact, to keep information for as long as they can because something that may not be useful today to extract information that could be useful for marketing purposes or for some other purpose, might be useful in the future using the analysis technology that is developed in the future.

So without those principles that require minimization of data and require limits to retention, as well as strong enforcement authority that would cause entities holding data to fear the repercussions of keeping information for too long, then that practice is likely to continue.

Senator HASSAN. Well, thank you.

Thank you, Mr. Chair.

The CHAIRMAN. Thank you, Senator Hassan.

Senator Cortez Masto.

STATEMENT OF HON. CATHERINE CORTEZ MASTO, U.S. SENATOR FROM NEVADA

Senator CORTEZ MASTO. Thank you. I also echo my colleagues; thank you for having this hearing, Mr. Chair.

And thank you for all of you being here today.

I want to follow up on a question I actually asked the last panel, and you touched on it, Mr. Mactaggart. This is the idea that the tough question for Congress right now, as we draft this privacy law, is how we define sensitive information versus non-sensitive information.

I asked that question to the panelists and you are absolutely right. They all kind of defined it a little bit differently. It would help me if you could give us a better understanding.

In California the law, I understand, eliminates the idea that sensitive versus non-sensitive distinction for the law's notice and opt-out requirements.

Can you talk a little bit more about that, how you have done that?

Mr. MACTAGGART. Essentially, we just treat all personal information the same, and we give consumers the control over it by saying, "You can chose who to do business with."

What we found in our research, what bothered consumers is the sense that that is being transferred and sold to companies they have never chosen to do business with and that they have no knowledge of.

I think one of the things that Ms. Moy just touched on is information changes over time. So what was not sensitive, now becomes sensitive because now you can do something with it.

What we basically say is, "All information, you shall have control over," but we kind of respect the consumers to understand that they are going to do business with a company, so that first party relationship is where we end up drawing that line.

Senator CORTEZ MASTO. Would this also, then, address the concerns that I heard earlier, I think it was the Chairman, about the customer loyalty programs? This would be information, then, that the customer would decide that they want to share with those programs and it would not get caught up in whether it is personal information or non-personal information, sensitive or non-sensitive. It is a broader category.

Mr. MACTAGGART. Right, because the customer is deciding to do business, yes.

Senator CORTEZ MASTO. Right. And it is up to the customer to make that determination. Got it.

The other area that I am interested in hearing a discussion on is the idea about data minimization, and I think it goes back to what, I believe it was Senator Markey, talking about the flashlight application example.

I understand one component of the GDPR is a concept called data minimization, and it is just what, I believe, Ms. Moy talked about. The principle states that data processing should only use as much data as is required to successfully accomplish a given task. Data collected for one purpose cannot be repurposed without further consent is my understanding.

I am going to ask Mr. Mactaggart, but Dr. Jelinek, if you would talk a little bit about how that is addressed in the GDPR, the data minimization, the implementation of it, I am interested in. How are smaller entities dealing with this provision?

Mr. MACTAGGART. Senator, I went into Super Cuts last week to get ready for this. Since the time I went to this haircut from the last time, Super Cuts now has a little kiosk.

They wanted my e-mail address and my cell phone number to check-in and I was the only person in line. The data collection has just gone out of control. I think that is one of the reasons why we are here because Americans have no certainty about where it is going, who is buying it. We do know it is getting stolen with regularity. I think the CCPA provides a meaningful approach to that.

Senator CORTEZ MASTO. Thank you.

Dr. JELINEK. The GDPR addresses that you just have to process the data when needed for the treaty you are working on.

If you just need the minimum data and if you just process the minimum data, which is provided in the GDPR because that is one of the core principles that you have to minimize the data. You do not have to have the data or some other thing.

If you just have a treaty regarding you buy a car. So you just have to provide the data regarding this treaty and not any more.

Senator CORTEZ MASTO. And so, do you then rely on those companies to self-regulate, and if they are somehow caught doing more, then that is where the enforcement comes in, and robust enforcement like I heard? I think it was Ms. Moy talked about the need for.

Dr. JELINEK. This robust enforcement can take place, yes.

Senator CORTEZ MASTO. OK. I know I only have a few minutes left.

I am also interested in the idea of this enforcement because I do believe there is the opportunity to self-regulate and then how we look at what enforcement is necessary.

I agree, I do not think it should be one-size-fits-all. I think in this Committee, you have former attorneys general. I think there is a dual role here where we can work together at the Federal level with the FTC along with the AGs.

The reason why I say that is because I know there are cases at the FTC may take and may not take that are necessary for individual states to address that will not be addressed if we just leave it to the Federal authorities. I also know there is an opportunity for both to work together.

The one thing I would caution, however, is not all AGs are the same and their authority is not the same. So the Attorney General

in California has regulatory making authority; the AG in Nevada does not. So as we go down this path, we really have to understand that enforcement piece of it, but I agree. I think there is a role for us to work together.

So my time is up, but I would love, and I have further questions on this piece of enforcement and how you think there is this dual role, and still not over enforcement and over regulation of the company, so they can still be free to innovate and be successful in their businesses as well.

Thank you. I know my time is up.

The CHAIRMAN. Thank you, Senator Cortez Masto.

Senator Young.

STATEMENT OF HON. TODD YOUNG,
U.S. SENATOR FROM INDIANA

Senator YOUNG. Well, thank you, Chairman.

I want to thank our panelists for being here today.

One of the areas I would like to touch on in this important discussion about privacy is the insufficient, at least as compared to previous generations, number of startup companies that we see being created.

Much has been written about this, and this exists within the Internet ecosystem, and certainly outside of it as well. But regulations, particularly those regulations that are somewhat hard to understand and may be difficult to comply with, tend to be favored by incumbent firms in any industry. It is just economic incentives dictate that.

That raises some concerns I have with respect to GDPR and the approach that is taken there and potentially by California. I will just start with Dr. Jelinek.

Perhaps to a greater degree than under the E.U.'s regulatory model, the United States, we tend to adopt a somewhat more flexible regulatory approach by my observation, by reputation certainly, than the E.U. does. There are advantages and disadvantages to that approach.

Do you have concerns that startups, in particular, might suffer under the approach the GDPR has taken? And if so, what steps are you taking or will you take moving forward if you discover that startups are being stifled by the approach the GDPR has taken?

Dr. JELINEK. Thank you, Senator, for this question.

I think just for startups, and assuming it is the GDPR, it is good because if they are just at the beginning of their business, they can already take into account rules and adapt from the beginning on through privacy policy by design, privacy policy by default.

They think this is really for the small SMEs and startups, if they just take into account from the beginning the rules of the GDPR, if they start when inventing a new processing or things like that.

They can rely on the robust, modern like the GDPR when they want to do business in Europe too. They can do it through the same rules in all of Europe and they do not have to be compliant to 28 different laws just to be compliant to one, to the GDPR, and that is quite easier also for small businesses.

Senator YOUNG. Is it not, moving forward, a real advantage to incumbency here, though? Because if your business model is to

maximize profit through the sale of advertisement, you already have tens of millions of users out there, and are enjoying all the revenue advantages of having those existing users, and the network effects associated with those users. Then you have established a new regulatory regime like GDPR or perhaps the California model.

Are you not disadvantaging new entrants into the space? I am not saying that your approach is the incorrect approach, but I just would like to know how you have tried to navigate this.

Dr. JELINEK. I think I made this clear. I think it is really an advantage for new businesses to have a robust set of rules for all Europe if they want to make business there.

Senator YOUNG. OK. Mr. Mactaggart.

Mr. MACTAGGART. Senator, I think, one of the reasons we decided to set the threshold at a high revenue, $25 million, is by definition, you exclude startups. They are not covered nor are the mom and pops, which is the backbone of the economy.

I feel if you are showing up, you are going to give the right to collect your information to the Google's, and the Amazon's, and the Facebook's because you already know them. The new company, it is going to be harder to compete.

So one of the reasons we put the line on the outside saying, "All companies have to give the consumer the right not to sell their data." But on the collection side, we were silent because we understand how does the next Google show up if no one is going to give their information to it in the first place?

Senator YOUNG. Sure. Ms. Moy.

Ms. MOY. Sure, just two quick points.

One is that, I think that this is one reason that rulemaking is really important to provide clarity in advance as well as State AGs which do a lot of important guidance.

Another really important thing to talk about is data portability, which helps new entrants to the marketplace.

Senator YOUNG. That is a good point. Yes.

Ms. O'CONNOR. I think it is incredibly important to be protective of the small business, but I would like to remind the Committee that Cambridge Analytica was a small business. The damage that can be done by small entities holding vast amounts of data is certainly equal to large entities holding vast amounts of data.

I would not exempt small entities from a baseline, comprehensive privacy law, but I would certainly be concerned about making sure the rules are clear, and simple, and provide direct guidance for all new entrants to the market. I am very concerned about the new entrants to the market, but I do not think the law should exempt them.

Senator YOUNG. Thank you.

The CHAIRMAN. Thank you, Senator Young.

Senator Udall.

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Thank you, Chairman Thune.

Since this Committee held a hearing to protect consumer data two weeks ago, consumers have already been subjected to two extraordinary data breaches.

I believe Chairman Thune mentioned one of them, Facebook. Hackers accessed 50 million Facebook users, although Facebook still does not know who the hackers are and which accounts were hacked. Google just disclosed this week a security flaw that it discovered in March that affected hundreds of thousands of people using its Google Plus social network.

It seems like hardly a week goes by that there are not new examples of how tech companies are just not doing enough to protect consumer privacy.

In our last hearing, I raised the issue of this in terms of children. Parents often trust these platforms with their children's information. As part of this privacy discussion, we must prioritize protecting children in this increasingly online world.

This question is to Ms. Moy and Ms. O'Connor. The nature of the Internet has evolved from a keyboard, to mobile devices that fit in our pocket, to the current day iteration of voice interface.

Is COPPA an example of the regulation that has adapted with the rapid evolution of technology? How has this law succeeded in keeping up with these changes and how has it failed?

Ms. MOY. Thank you.

The Children's Online Privacy and Protection Act, I do think that one thing that is really great about that Act is that it gave rulemaking authority to the Federal Trade Commission. The Federal Trade Commission did expand the definition of personal information in its implementing rule in 2012 in an attempt to keep up with rapidly advancing technology.

I agree that additional protections may be needed for children in the modern era. That said, I do think that COPPA has proven itself to be a pretty flexible law.

Senator UDALL. Ms. O'Connor.

Ms. O'CONNOR. Thank you, Senator.

As a mother and soon to be stepmother of six children ranging from 9 to 19, I feel strongly about the stepped up nature of the use of the Internet from the youngest to the oldest teenager and so on.

COPPA certainly has its strengths and it has been effective in its enforcement by the Federal Trade Commission, but as you know, it stops at 13 and there is a big gap between the young teen and the adult. We need to explore what that world looks like for those in transition from teenage to adulthood.

We also, as you correctly point out, are moving from a world where the Internet was something you sat down to do at your computer, to carry around to your phone, to embedded in the walls of your house, and your school, and your car.

We are particularly concerned at the Center for Democracy & Technology about the use and collection of data in schools by for-profit companies and by other entities, and what that kind of data determinism looks like as kids apply to college and beyond.

Senator UDALL. Thank you very much.

This question is to the entire panel. A recent *New York Times* analysis found that both the Apple App Store and the Google Play

Store have applications in their respective children or family sections that potentially violate COPPA.

What specific role should platform owners play to ensure compliance on their platforms?

Mr. MACTAGGART. Senator, in the hearing two weeks ago, the representative from Google said that they relied on the application developers to tell them whether or not it was a child-directed app, and they relied on the app developers to self-certify.

This is, I think, a good example of the fact you need really robust enforcement. It is like waiting for the cops, to call the cops and tell them you have been speeding. It does not work, sir.

Senator UDALL. What would you do in Europe with this kind of situation?

Dr. JELINEK. In Europe, with this kind of situation, it depends. The controller cannot rely on the application developer because the controller is responsible for what he is doing and for what he is providing. If there are problems regarding children, and there are complaints, and also if there are no complaints because we can have investigations ex officio, we are going to investigate those cases.

Ms. MOY. There are a couple of things that have proven problematic.

One is that there are incentives set up essentially for those that have app stores to essentially just have no knowledge of whether or not apps on their platform are directed to children. That is a gap that should be fixed.

I have lost my second point.

Ms. O'CONNOR. Well, we certainly think that the immediate company, the app developer or owner, is the ultimate responsibility. We certainly would look at what kind of compliance mechanisms exist for the larger platforms to take action against those companies that they become aware of that are not compliant.

Senator UDALL. Thank you. My time has expired.

Thank you, Mr. Chairman, for really focusing in on this and having the number of hearings.

The CHAIRMAN. Appreciate that. Thank you, Senator Udall.

Senator Schatz.

STATEMENT OF HON. BRIAN SCHATZ,
U.S. SENATOR FROM HAWAII

Senator SCHATZ. Thank you, Mr. Chairman.

Thank you all for a great panel. I really appreciate the plainspokenness of your expertise. It is really useful for the general public because this really does matter to a lot of people.

As I mentioned in the previous hearing, the reason we are having a more robust, more serious conversation about a Federal privacy law is that there is this California privacy law, and it is forcing folks to the table that have been, so far, hesitant to have this conversation about a Federal law.

My analysis, and it is informed by what I am starting to hear, is that some of the tech companies are really serious and want to do this, and want to do this regardless of whether or not the California law gets amended. Others are trying to figure out where and how they can do the minimum; which is to say, if they can get the

California law weakened, then they are going to back off of their support for a Federal privacy statute.

And so, I want us all to not pretend not to know that that is happening. That is exactly what is happening. That is the context in which this negotiation is occurring. And so, let me just go down the line.

The first question, in my view, is the FTC's rulemaking authority. You cannot really have a law in this space without the FTC's ability to be the expert agency and to enforce.

Do you think a Federal privacy law ought to have FTC rulemaking authority? Starting with Dr. Jelinek.

Dr. JELINEK. I have to tell you that is a decision of the U.S. lawmakers.

Senator SCHATZ. Well, that is fair enough. Thank you. That was actually my thought, but I wanted to be inclusive because I did not want to skip you. Thank you.

Ms. MOY. Yes, absolutely essential.

Ms. O'CONNOR. Yes, and direct fining authority, not reliant on consent decree.

Senator SCHATZ. Can you flesh that out a little bit, Ms. O'Connor?

Ms. O'CONNOR. Sure. I have actually worked once at a company that was under investigation by the FTC, so I am well aware of the zealousness with which they pursue their action.

They are a terrific agency with really talented staff. Not enough of them, only 60 staffers for the entire United States working on data privacy in particular and reliant on the FTC's Section 5, Unfair and Deceptive Acts and Practices provisions. That is not a direct enough instruction to the agency.

That is why the body needs this law to say, "This is what is in and this is what is out for companies. This is what is allowed and what is not." But they have to wait until they find a malicious or untrue statement in a privacy policy, then take action, then have a consent order, and then find a violation of that. That is a lot of time and water under the bridge.

Senator SCHATZ. Because as you are balancing what your general counsel says, versus what your coders say, versus what your shareholders want, you just say, "Why do we not just run this and figure out how much trouble we are going to get in, in 3 years once we are ten times as large?" Right?

Ms. O'CONNOR. And having worked in some of these companies, the engineers and the computer scientists tell me, "Just tell me what the rule is. I want one, clear rule. I want to understand what I am expected to do, and I will code to that. I will fix that. I will make that happen."

But waiting until we test what the boundaries of harms are is not working for consumers in this country today.

Senator SCHATZ. Ms. Moy, Mr. Mactaggart, anything to add to that?

Ms. MOY. Yes, I will just add that I agree completely, of course, that fining authority is needed for the FTC, and it must be substantial penalties. Under the GDPR, I think that the penalty can be up to 4 percent of a corporation's annual revenue.

The penalty against Google in 2012 for violating its consent decree was only $22.5 million and that was just a few hours of revenue for that company.

So not only must there be penalties or fining authority for the FTC, but also those fines must be substantial, such that they can actually raise privacy concerns to a CEO level concern instead of just something that the tech folks at the firm are looking at.

Senator SCHATZ. Mr. Mactaggart.

Mr. MACTAGGART. I just agree with everything that has been said. You need trust and check, and the check part needs to have some stick to it as well.

Senator SCHATZ. Let me start with you, again, Mr. Mactaggart.

Tech and telecom are in a fight about who is supposed to comply with what privacy laws. There are no angels. God bless them all. We have working relationships with all of them, but there are no angels. They want rules for the other, but not for themselves.

I wonder if you would not mind just spending a minute or half a minute talking about the need for whatever we do as Federal law to apply across platforms and business models?

Mr. MACTAGGART. Yes, I just think any Federal legislation needs to be strong, effective, and meaningful. As has been said before, you do need a robust enforcement mechanism. I can see why the companies want this, but I think what you said is exactly right.

My experience just even in the clean up bill in August in California was that there were a couple of tiny, little words inserted that they tried to say, "This is just clarification," and then the reality is if we would have let those stay that would have totally gutted the law. They have the smartest lawyers in the world pushing hard.

So that is what is going to happen. They are going to try to deal with California first and if they do not get it, they will try to come here.

Senator SCHATZ. Thank you.

The CHAIRMAN. Thank you, Senator Schatz.

Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman.

Thank you for holding this hearing and the witnesses. I thank Senator Schatz for his questioning because it is along the lines of what I wanted to ask about.

I used to say that we were just at the tip of the iceberg of the Information Age. Now, I am pretty sure we have looked under the waterline and seen this massive amount of data information, application integration, and opportunity. But now I am pretty sure we have a good sense of how big the Information Age really is and the implications for us.

Every day, we see threats of cyber security, not just companies being hacked, but state actors causing great concern as they look at our power plants or electricity grid. All of this is incredibly important.

I feel like the panel is presenting two different opportunities here. Either the GDPR model or we get the FTC, as you just all

advocated, to have fines and regulatory authority in a broader fashion. So I appreciate that.

I would ask about the fact that we did not really, my colleague did not really clarify, but if you could clarify because we talk about the misuse of data on the OPM or Equifax issue which, to me, is always amazing. Again, because Equifax there was a patch that just had to get done and somebody did not do it.

So this whole issue of hygiene is something that we work really hard on in the State of Washington trying to clarify with our National Guard and everybody else. These are the basics of hygiene that you need to be doing every day to protect your business, your home, devices, what have you. But misuse of data is also a concern, so not just the theft of somebody leaving you vulnerable, but the actual misuse of data.

Should that be covered under those FTC fines or regulations? Could you comment on that?

Ms. O'CONNOR. In our proposals that we are working on with a member of your staff, and I thank you very much for that, we are particularly concerned about secondary uses or extraneous uses of the data when collected for one purpose, but then used by the same company for another purpose, particularly if that data is highly sensitive, biometric, or children's, or health indicators.

We are also obviously concerned about third-party transfers and uses that were unexpected to the individual consumer.

I think you are so right to make the point that this is a larger ecosystem. It is not only about technology companies or telecom companies. Data is flowing on and offline through traditional companies and tech companies.

Our phrase, really, is everybody in the pool. This is a law that is about the individual and their rights and their data, no matter where it flows in the ecosystem.

Senator CANTWELL. Thank you.

Ms. MOY. I just want to clarify that I think that both approaches are ultimately necessary. Both are baseline.

Both baseline privacy that are based on, that comes from a place of principles, as well as increased authority for an expert agency in the form of rulemaking, civil penalty authority, and greater resources.

But then, I also think that we may need heightened protections as it relates to things on your question of uses that might be prohibited. I think, as I mentioned in my testimony earlier, information about consumers should not be used to discriminate against them. Right? Information about consumers should not be used to deny access to or just awareness of opportunities that relate to things like education, finance, and health care.

Right now, that is going on and I think that we need more than just privacy to deal with that. We need regulations that prevent use of information for those purposes or, at the very least, that create greater protections around it and greater transparency about how information may be used for those purposes, and accountability for consumers.

We may need heightened standards as well in other areas, as my colleagues have mentioned, heightened standards around children's

information, heightened standards around biometric information, et cetera.

Senator CANTWELL. What about election meddling? I am reading these stories now about this Israeli company that was promoting these concepts of, "Here is what you could do."

What do we do about that disclosure?

Ms. MOY. That is obviously an extremely difficult problem that I do not think there is any easy solution to.

I think in the near term, we certainly do need greater information about how data is being used to target not only advertisements for specific political candidates, but information that relates to issues of central importance in elections that may sway voters' decisions.

We need greater transparency so that researchers can get in there, and study it, and find out the extent to which this information manipulation is changing voters' behavior because it surely is.

Senator CANTWELL. Mr. Mactaggart, do you have any comments on that?

Mr. MACTAGGART. I would just add, I think there is nothing more important for this Committee to focus on. Someone talked about oil before. Standard Oil was powerful. They did not know everything about you.

We have never before had a situation where companies know everything about you intimately and can communicate to you at essentially zero cost. This is a new technology. It is a new thing and there is nothing more important for this committee to consider.

Senator CANTWELL. Why, thank you. I know I am a little bit over, Mr. Chairman, but I think one of the witnesses said it best. This Committee is here to protect these consumer rights. So often, this Committee is engaged in the arbitration between behemoths in a tech sector or maritime or aviation, whatever it is. But here, we have to remember our duty and responsibility to protect consumers on their privacy rights that, I believe, are very strong in our Constitution.

Thank you.

The CHAIRMAN. Thank you, Senator Cantwell.

Senator Duckworth.

STATEMENT OF HON. TAMMY DUCKWORTH, U.S. SENATOR FROM ILLINOIS

Senator DUCKWORTH. Thank you, Chairman Thune and Ranking Member Nelson for holding this important meeting.

I would also like to thank today's witnesses for an honest and frank discussion.

The reality is that the Federal Government has fallen behind the curve in protecting digital security rights, and as an online shopper, in fact as a mom of two girls under the age of four, if it does not come from Amazon, then I am not getting it. It is just the way it is.

I recall receiving various notices and disclosures from technology companies highlighting changes to their policies and procedures in order to comply with the European General Data Protection Regulation, as did most online consumers.

As a U.S. Senator, I was really struck by how these actions shined a spotlight on Congress, our Congress' failure to modernize Federal privacy laws and regulations. I would also notice that despite the alleged stifling impact of the E.U.'s comprehensive regulation by some, the sky has not fallen in Silicon Valley and technology giants continue to grow and thrive.

Ms. O'Connor, Federal agencies within the U.S. Department of Commerce, specifically the National Institute of Standards and Technology and the National Telecommunications and Information Administration, have begun to develop a privacy framework to help address risk and build trust between industries and individuals.

At a recent Brookings Institution forum, the Director of the National Institute of Standards and Technology highlighted the industry's preference for a light touch regulatory approach and suggested that it is too soon to determine the impacts of the GDPR and the California law would have on privacy outcomes.

At the same time, he also questions each law's sustainability. So he said it was too soon for us to look at how effective the GDPR is or how California would be on policy outcomes.

So my question is, I am not asking you to get into the mind of the NIST Director, but from a practical standpoint, how does one gauge the impacts of GDPR and CCPA on products and services that require use of data?

Ms. O'CONNOR. Thank you so much, Senator.

I was not there for that comment, but I would say that we are 25 years on from the dawn of the commercial Internet. I think we have tried self-regulation. I think companies have flourished. I do not think it is too soon to consider this question.

I think it is high time, if not past time, to consider how we protect your and my children and all Internet consumers in the future generation. I do not think we can wait another 25 years to regulate.

Do we think that there are challenges with the GDPR approach? We think the values, both in the GDPR and in the CCPA, are sound and they reflect the primacy of the individual and their interests in their data.

Do we think, perhaps, there is a lot of notice and maybe not strong enough boundaries about what kind of data should be in or out of bounds for companies to use? Certainly, these are questions for this body to consider, but I think the values are sound, and I think we are, if anything, late to the party.

Senator DUCKWORTH. Well, so it is too soon, though, for us to be able to measure the improvement or on privacy outcomes from the GDPR? I feel like people are saying it is too much. There is not enough good coming out of it. But I feel like it has just been implemented.

Is that an accurate assessment?

Ms. O'CONNOR. I think that is a fair comment to say. I misunderstood, perhaps, and thought you meant it was too soon to regulate. It is probably too soon to judge what he eventual outcome and challenges are to companies doing business inside or outside Europe.

But the fundamental values of respect and dignity to the individual, of allowing them the transparency, allowing them the data portability particularly, which Laura and others have mentioned,

allowing more power in the hands of the individual vis-á-vis a large institution actually rebalances the power equation. I think that favors, in fact, small and startup businesses over incumbents, or at least levels the playing field a little bit more.

So a clear, simple standard for U.S. companies to know what they are allowed to do with our regular or personal data or sensitive data is a good move.

Senator DUCKWORTH. So then, how would one gauge the sustainability of any type of privacy framework that we can come up with?

Ms. O'CONNOR. Well, Europe has had a Data Protection Directive for 20-something years.

In the United States, we have had a sectoral approach and we can certainly look at what kind of successes, or failures, or challenges we have had in our health privacy laws, in our financial institutions' laws, in our children's privacy laws. I think we can build upon those without weakening those standards and take the best from each of our frameworks.

But I think most importantly for companies of all sizes, clear direction about what they are allowed to do with, and to, consumer data that they collect in the ordinary course of business is necessary.

Senator DUCKWORTH. Thank you.

I yield back.

The CHAIRMAN. Thank you, Senator Duckworth.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

Thank you to all of you. I had another hearing in between here.

I want to also thank Senator Markey.

I think you all, probably, everything has been said, but I have not said it yet. So we have had a very, I would say, watershed year that we have never seen before when it comes to consumer privacy where people are finally coming to grips with this.

Just last week, we saw additional data breaches at Google and Facebook that exposed the personal information of millions of customers.

Senator Kennedy and I have our Social Media Privacy Protection and Consumer Rights Act, which I think just has some baseline protections. Thank you for nodding your head, Ms. O'Connor. It is a bipartisan bill.

A few things. Ms. O'Connor, do you believe there is a need for this kind of legislation? What consequences do we face if we do not have some kind of privacy law in place?

Ms. O'CONNOR. Thank you so much, Senator Klobuchar, for that question, and thank you for your leadership on this issue.

I was nodding because we do, obviously, applaud and support the principles ensconced in your legislation. I would simply like to see legislation that affects and impacts all commercial entities across the United States, regardless of what sector they self-describe themselves to be in.

When I am doing business online or off, I do not necessarily know the company I am doing business with is governed by the

Telecom Act, or HIPAA, or COPPA, or whatever the patchwork of laws that we have at the Federal level is. I simply know that I want to get the goods or service in front of me. I want to know that my data is not going to be used in ways that far exceeds my expectation about the transaction in front of me. I want to know that the data is secure. So yes, I think it is high time.

Senator KLOBUCHAR. Dr. Jelinek, can you explain why the GDPR includes the 72 hour notification window? We have that as well in our bill, but can you explain it?

Dr. JELINEK. As I mentioned before, I was not negotiating the GDPR.

But as far as I see, the 72 hours of notification of a data breach, another problem for the companies, because if the data breach occurs they just know it and they have to report it to the data protection authorities. And the first notice does not have to comprise everything because they have to investigate too.

And until now, the 72 hours whenever the problem, the problem is if someone wants to hide that there was a data breach, and then you can have 1 week, 2 weeks, or three weeks. If they do not want to tell you, that is a problem. Not the 72 hours.

Senator KLOBUCHAR. Can you explain how Europe has approached the concept of withdrawing consent, someone consents to have their information used, and they changed their mind? How important do you believe that this protection is to be able to give them that right?

Dr. JELINEK. This protection is not a new one. This was already a right under the Data Protection Directive. But consent is only one point which is possible to give because you can rely on law if you are processing data or lets you admit interest. And so, consent is not always the point.

But when you have the free will and you have the consent, then you can withdraw the consent. Until now, the withdrawal of the consent has never been a problem during the last 20 years of the Data Protection Directive. And I think there will not be any problem regarding the GDPR regarding this point.

Senator KLOBUCHAR. OK. Ms. Moy, the bill I wrote with Senator Kennedy preserves the rights of State Attorneys General to take action against companies when privacy violations occur.

What role do you see those attorneys general, what they can play in policing online marketplace? How does their authority complement the FTC?

Ms. MOY. Great, thank you for that.

So State attorneys general, they do a number of very important things, but a couple that I would like to highlight are, one, State attorneys general can take action when they are dealing with small cases that may not rise to the size or number of consumers affected that would trigger enforcement action on the part of a Federal agency.

The Federal Trade Commission does a lot of work on data security right now, but it only has a staff, I think, of around 1,100 people and there are thousands of breaches that take place at a small level that may only affect hundreds of consumers at the State level. State attorneys general are doing really, really good work there.

State attorneys general are also doing great work consulting with businesses and stakeholders in their communities to try to provide the necessary guidance that companies need to understand what their obligations are and that consumers need to understand what their protections are.

Senator KLOBUCHAR. Thank you.

I had a question for you, Mr. Mactaggart, but there is a glass ceiling and you did not make it through. I will give you one in writing.

Thank you.

The CHAIRMAN. Thank you, Senator Klobuchar.

We definitely want to protect the privacy of Green Bay Packer fans living in the State of Minnesota.

Senator KLOBUCHAR. Excuse me. Did you see that the Vikings beat the Super Bowl Champions this weekend? If you want to give Vikings grief, you did not pick the right week to do it.

Thank you.

[Laughter.]

The CHAIRMAN. Let me just direct this to Ms. Moy and Ms. O'Connor, just to wrap up. I think we have a vote on, actually, so we are going to have to head over to the floor here momentarily.

Are there provisions of the GDPR and the CCPA that you think we ought to include as we look at and contemplate Federal legislation? And are there specific provisions in either law that we ought to avoid or that need to be improved?

Ms. MOY. Sure. So I think a few things that I would highlight about the GDPR.

One, as I have mentioned before, the substantial fining authority such that fines really can rise to a level that provides the right incentives for companies under the GDPR and we desperately need that here in the U.S.

Another thing that I would highlight is this idea that consent, when it is given on the part of a consumer, must be freely given is something that is really important for us to incorporate into any principles that we have here in the U.S. because it recognizes that where a service is essential and unavoidable for a consumer, then consent might not be freely given.

It also recognizes that where consumers are charged a penalty for failing to provide their consent, then if that is a penalty that is coercive or if you are dealing with a consumer who simply cannot afford to pay that, then that might make consent also not be freely given. I think that that is something that is really important to consider.

Of course, the data minimization and purpose limitation principle is great as well. The GDPR really does have a lot going for it.

Ms. O'CONNOR. Both of the laws ensconce some basic data protection principles. There seems to be general agreement.

I am surprised to see companies agreeing with things that, 10 years ago, we would not have seen such widespread assent to notice, and choice, and access, and deletion, and correction, and most importantly, portability which allows the individual consumer control over their data. So the core values, I think, are largely consonant.

Where I think we do not see enough is in guidelines and bright line rules in the GDPR about what should not be done and what kind of data should not be collected and used.

And while on CCPA, there are drafting and definitional questions, we have an annotated version of the bill on our website at *CDT.org*. We think that the values are sound and the enforcement mechanisms are sound. We want to see coverage for all entities, large and small, because we think there could be tremendous damage even from small companies' use of large amounts of data.

We want to see clear guidance and delineation of secondary uses and third-party uses. But overall, we are supportive and we do not want to see those protections weakened.

The CHAIRMAN. Last week or two weeks ago when we heard from the leading global technology firms, the testimony was that some companies are having to devote huge resources in order to comply with the GDPR.

Can you describe for us what the average GDPR compliance costs are for companies, Dr. Jelinek?

Dr. JELINEK. Mr. Enright was quoted that Google had to spend hundreds of manpower years to be compliant with the GDPR.

If you take into account that Google has, according to the latest figures, 85,085 people, and you take 200 years, then one employee of Google has not spent more than three-and-one-half hours for compliance with the GDPR. That is the first.

The second is, I think, if these tech companies would have been compliant before with the Data Protection Directive, they would not have had to invest so much money because, as I said before, GDPR is no revolution, but just an evolution.

Most of the tech companies really tried to be compliant and develop robust systems regarding their customers.

But as we hear every week, there are data breaches and other things that occur. I think this addresses very good and very well how important the GDPR is and the provisions for the consumers, for the individuals.

The GDPR gives back to the individuals the control over their personal data because they have the right to free consent, the right of access, the right of deletion, and some other rights which are core principles of the GDPR.

As already said before, I think Americans do not deserve less protection than the Europeans. Thank you.

The CHAIRMAN. Great. We will probably have other questions, which we will submit for the record and we would ask if you could get those responses back as quickly as possible to members of the Committee. We will keep the hearing record open for a couple weeks in order to allow for that.

We greatly appreciate your time.

Senator MARKEY. Mr. Chairman.

The CHAIRMAN. Yes.

Senator MARKEY. Can I just compliment you on the uniformly excellent testimony from each one of the witnesses. It was really an extremely high quality panel, and I want to congratulate you on that, and to the witnesses yourselves.

Thank you.

The CHAIRMAN. Thank you, Senator Markey.

Yes, we got lots of good input and responses to questions, which will help us as we make decisions going forward. Thank you all very much.

We will keep the record open, as I said, for a couple of weeks. But with that, this hearing is adjourned.

[Whereupon, at 11:54 a.m., the hearing was adjourned.]

A P P E N D I X

CONFIDENTIALITY COALITION
October 10, 2018

Hon. JOHN THUNE,
Chairman,
U.S. Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Hon. BILL NELSON,
Ranking Member,
U.S. Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

The Confidentiality Committee applauds the U.S. Senate Committee on Commerce, Science, and Transportation's efforts to examine consumer data privacy.

We are broad group of organizations-hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, clinical laboratories, patient groups, home care providers, and others-working to ensure that we as a nation find the right balance between the protection of confidential health information and the efficient and interoperable systems needed to provide the very best quality of care.

The Health Insurance Portability and Accountability Act {HIPAA) established acceptable uses and disclosures of individually-identifiable health information within healthcare delivery and payment systems for the privacy and security of health information. The Confidentiality Coalition believes that to the extent not already provided under HIPAA, privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information. As the Committee explores consumer data privacy in the context of the European Union's General Data Protection Regulation and the California Consumer Privacy Act, the coalition encourages a privacy framework that is consistent nationally and includes similar expectations of acceptable uses and disclosures for non-HIPAA covered health information, as it is paramount to maintain consumer trust.

Thank you for examining this important issue and please feel free to reach out to Tina Olson Grande, Senior Vice President for Policy at the Healthcare Leadership Council on behalf of the Confidentiality Coalition, at (202) 449–3433 or *tgrande@hlc.org* with any questions. Enclosed you will find information on the Confidentiality Committee and a list of coalition members.

Sincerely,

TINA OLSON GRANDE,
Healthcare Leadership Council,
on behalf of the Confidentiality Coalition.

ABOUT THE CONFIDENTIALITY COALITION

The Confidentiality Coalition is a broad group of organizations working to ensure that we as a nation find the right balance between the protection of confidential health information and the efficient and interoperable systems needed to provide the very best quality of care.

The Confidentiality Coalition brings together hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, clinical laboratories, patient groups, and others. Through this diversity, we are able to develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

We advocate for policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, supporting policies that enable the essential flow of information that is critical to the timely and effective delivery of healthcare. Timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

Membership in the Confidentiality Coalition gives individual organizations a broader voice on privacy and security-related issues. The coalition website, *www.confidentialitycoalition.org,* features legislative and regulatory developments in health privacy policy and security and highlights the Coalition's ongoing activities.

For more information about the Confidentiality Coalition, please contact Tina Grande at *tgrande@hlc.org* or 202.449.3433.

MEMBERSHIP

Adventist Health System
Aetna
America's Health Insurance Plans
American Hospital Association
American Pharmacists Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
Athenahealth
Augmedix
Bio-Reference Laboratories
BlueCross Blue Shield Association
BlueCross BlueShield of Tennessee
Cardinal Health
Change Healthcare
CHIME
Cigna
City of Hope
Cleveland Clinic
College of American Pathologists
ConnectiveRx
Cotiviti
CVS Health
dEpid/dt Consulting Inc.
Electronic Healthcare Network Accreditation Commission
Express Scripts
Fairview Health Services
Federation of American Hospitals
Franciscan Missionaries of Our Lady Health System
Genetic Alliance
Genosity
Healthcare Leadership Council
Hearst Health
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
LEO Pharma
Mallinckrodt Pharmaceuticals
Marshfield Clinic Health System
Maxim Healthcare Services
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medidata Solutions
Medtronic
MemorialCare Health System
Merck
MetLife
National Association of Chain Drug Stores
National Association for Behavioral Healthcare
NewYork-Presbyterian Hospital
NorthShore University Health System
Novartis Pharmaceuticals
Novo Nordisk
Pfizer
Pharmaceutical Care Management Association
Premier healthcare alliance
Privacy Analytics
Sanofi US
SCAN Health Plan
Senior Helpers
State Farm
Stryker
Surescripts
Texas Health Resources
Teladoc
UCB
Vizient
Workgroup for Electronic Data Interchange
ZS Associates

PRINCIPLES ON PRIVACY

1. Confidentiality of personal health information is of the utmost importance in the delivery of healthcare. All care providers have a responsibility to take necessary steps to maintain the trust of the patient as we strive to improve healthcare quality.
2. Private health information should have the strictest protection and should be supplied only in circumstances necessary for the provision of safe, high-quality care and improved health outcomes.
3. The framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule should be maintained. HIPAA established a uniform framework for acceptable uses and disclosures of individually-identifi-

able health information within healthcare delivery and payment systems for the privacy and security of health information.
4. The Privacy Rule requires that healthcare providers and health plans use the minimum necessary amount of personal health information to treat patients and pay for care by relying on patients' "implied consent" for treatment, payment of claims, and other essential healthcare operations. This model has served patients well by ensuring quick and appropriate access to medical care, especially in emergency situations where the patient may be unable to give written consent.
5. Personal health information must be secured and protected from misuses and inappropriate disclosures under applicable laws and regulations. Strict enforcement of violations is essential to protect individuals' privacy.
6. Providers should have as complete a patient's record as necessary to provide care. Having access to a complete and timely medical record allows providers to remain confident that they are well-informed in the clinical decision-making process.
7. A privacy framework should be consistent nationally so that providers, health plans, and researchers working across state lines may exchange information efficiently and effectively in order to provide treatment, extend coverage, and advance medical knowledge, whether through a national health information network or another means of health information exchange.
8. The timely and accurate flow of de-identified data is crucial to achieving the quality-improving benefits of a national health information exchange while protecting individuals' privacy. Federal privacy policy should continue the HIPAA regulations for the de-identification and/or aggregation of data to allow access to properly de-identified information. This allows researchers, public health officials, and others to assess quality of care, investigate threats to the public's health, respond quickly in emergency situations, and collect information vital to improving healthcare safety and quality.
9. To the extent not already provided under HIPAA, privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information. A similar expectation of acceptable uses and disclosures for non-HIPAA covered health information is important in order to maintain consumer trust.

NATIONAL RETAIL FEDERATION
Washington, DC, October 10, 2018

Hon. JOHN THUNE,
Chairman, Committee on Commerce, Science, and Transportation,
United States Senate,
Washington, DC.

Hon. BILL NELSON,
Ranking Member, Committee on Commerce, Science, and Transportation,
United States Senate,
Washington, DC.

RE: *Hearing on Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act*

Dear Chairman Thune and Ranking Member Nelson:

The National Retail Federation appreciates your leadership on data privacy issues and applauds your holding of today's hearing on consumer data privacy issues to examine the lessons learned from the General Data Protection Regulation (GDPR) adopted by the European Union (EU), which took effect on May 25, 2018, and the California Consumer Privacy Act, which was enacted on June 28, 2018, and subsequently amended on August 31, 2018.

We have worked closely with our members on both of these data protection regulations, and below we share some of the lessons learned from each for your consideration. We view these recent engagements as part of a continuum of activity to help the retail industry develop best practices on data privacy and security matters over the past two decades. We have similarly worked with members of this Committee on related legislation during the same time, and we look forward to continuing our important collaboration with members of Congress to help develop Federal privacy legislation that the retail industry could support.

NRF is the world's largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the Nation's larg-

est private-sector employer, supporting one in four U.S. jobs—42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the Nation's economy.

Retailers' Use of Customer Data and Interests in Protecting Consumer Privacy

Protecting consumer privacy is one of retailers' highest priorities. Retailers know that establishing long-term relationships with their customers requires more than just providing the merchandise they want at the prices they are willing to pay. Successful retailers win their customers' trust and provide a satisfying shopping experience so that consumers continue to shop with them time and again. A critical element of establishing that trusted relationship lies in how retailers act as stewards of the information their customers share with them when shopping.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations for service. Whether online or in store, retailers use data to provide personalized experiences that consumers value. Customers, in turn, expect retailers to process their personal information responsibly and seamlessly when they are shopping. To meet these high expectations, retailers invest in technology and often spend many years developing methods to comply with state, Federal and (increasingly) global regulations on data usage in ways that further their customer relationships and does not frustrate them.

In short, retailers use customer data for the principal purpose of serving their customers as they wish to be served; the data collection is not an end in itself, but merely a means to the end of improving customer service. This practice differentiates retailers' principal use of customer data from other businesses—typically third parties unknown to the consumer—whose principal business is to monetize consumer data by collecting, processing it and selling it to other parties as a business-to-business service. As members of the Committee craft Federal legislation, it is important to recognize the fundamental differences in data usage between businesses that are known to the consumer, and serve them directly, from those that traffic in their data without consumer knowledge.

In 2009, the Federal Trade Commission explained in its staff report on online behavioral advertising the distinct differences between "first-party" and "third-party" uses of data, particularly regarding consumers' reasonable expectations, their understanding of why they may receive certain advertising, and their ability to register concerns with, or avoid, the practice:

> For example, under the "first party" model, a consumer visiting an online retailer's website may receive a recommendation for a product based upon the consumer's prior purchases or browsing activities at that site (*e.g.,* "based on your interest in travel, you might enjoy the following books"). In such case, the tracking of the consumer's online activities in order to deliver a recommendation or advertisement tailored to the consumer's inferred interests involves a single website where the consumer has previously purchased or looked at items. Staff believes that, given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.[1]

Indeed, millions of Americans learned of the significant risks of harm to them personally that can flow from irresponsible data practices by third-parties who are unknown to them, as we saw in the well-publicized Cambridge Analytica and Equifax incidents during the past thirteen months.

Principles for Federal Data Privacy Legislation

NRF began working with our retail company members on best practices to protect customer privacy in the late 1990s, with initial efforts focused on developing prin-

---

[1] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), pp. 26–27, available at: *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf*

ciples that promoted transparency and customer choice. Over the two decades since, NRF has participated in efforts by several Congressional Committees in the House and Senate to develop Federal data privacy legislation. We have also submitted comments to the Federal Trade Commission (FTC) on a range of data protection issues as it explored the contours of the Commission's authority, under Section 5 of the FTC Act, to protect consumers' data privacy and ensure businesses employed reasonable data security practices.

American businesses today cannot solely concentrate on Federal and state data privacy regulations. Conceivably, a data regulation adopted halfway around the world may impact a U.S. business operating entirely within our national borders and employing only American workers. Retailers are not immune to the significant challenges described by global tech companies (in a previous hearing) to reconcile newly adopted and conflicting data privacy laws—from the EU's GDPR to California's CCPA. They are also acutely aware of the potential for 50 different U.S. states and untold foreign governments to propose new data regulations each year that have a global reach (like the nature of the data each law intends to regulate).

These proposed regulations, even if well-meaning, may ultimately make it impossible for businesses to use data as they should to serve their customers in the many ways consumers have come to expect, largely because of the risks companies could face in the form of significant government fines or business litigation if they misjudge how best to use data responsibly to serve their customers. In the end, it may be consumers who stand to lose the most if businesses cease to take advantage of technological innovations to better serve them out of fear of tripping over a hodgepodge of potentially conflicting state, national and multi-national regulations that each authorize excessive fines for non-compliance.

Retailers would like to avert a global data regulation train wreck and support a U.S. Federal solution to data privacy that would apply nationwide requirements *uniformly* across all industry sectors handling similar customer information. As the Committee reviews proposals, we would urge you to adopt several key principles that we believe are essential to Federal legislation in this area of the law:

- *Federal Preemption of Related State Laws:* Congress should create a sensible, uniform and Federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that all sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting related state laws is necessary to achieve this important, national public policy goal. Without effective preemption of state law, Congress would simply add another data privacy regulation to what may eventually become a 50-state regulatory regime, where the U.S. laws fall within a larger, unworkable global regulatory gauntlet for businesses as state, national and multi-national laws all potentially conflict. Congress's effort to bring sensibility and certainty to data regulation is as important to the future of e-commerce as maritime law was to trans-oceanic commerce centuries ago.
- *Uniform Application of Federal Law to All Entities:* Federal data privacy legislation should apply to all industry sectors that handle the same or similar consumer data, and Congress should not craft rules that are specific to any subset of industry or permit exemptions that pick winners and losers among competitive industry sectors. To protect consumers comprehensively, a Federal data privacy law should apply equivalent requirements to all industry sectors handling similar sensitive personal information.
- *Transparency and Legitimate Interest:* Federal legislation should promote well-understood fair information practice principles, such as transparency and consumer choice, with respect to sensitive customer data. Businesses handling such data should be transparent about their collection and use of sensitive data and should provide consumers with meaningful choices in how such data is used. Retailers support principles like the GDPR's "legitimate interest" concept as a lawful basis for processing sensitive customer data, which properly aligns consumer expectations with business needs by balancing a business's legitimate interest in processing personal information to serve its customers with the customer's interest in protecting her data from misuse. The legitimate interest basis provides the regulatory flexibility necessary to ensure that businesses can use consumer data responsibly in ways that avoid frustrating the customer experience with incessant requests for affirmative consent where it is unnecessary for lawful processing.

We have come to these conclusions on which principles are critical to a U.S. Federal data privacy law through our continuous work with member companies on both the GDPR and CCPA. As presaged by today's hearing title, there are certainly les-

sons to be learned from each of these laws: some areas of enlightened thinking that we support, such as the GDPR's legitimate interest basis for processing customer data, as well as areas of concern that we hope members of Congress will address as they find alternative methods to achieve the public policy ends of a Federal data privacy law. We address several aspects of the GDPR and CCPA below to inform members of retailers' views on each law as the Committee considers the testimony of other stakeholders offered at today's hearing.

Lessons Learned from the GDPR

With the GDPR taking full effect this past May, there are still many questions that remain about how the regulation applies to critical areas of retail business operations, such as: using customer data for improved service or promotional opportunities, managing customer information databases and loyalty programs, collecting customer consents, and honoring customer rights to erase data, port data to another business, or access their personal data held by a business.

A business does not have to be a large multi-national company to feel the regulatory impact of the GDPR. Retailers operating in the U.S. with websites, mobile apps and other digital platforms serving consumers with Internet access may face new compliance standards, increased liability for violations and more stringent enforcement. While the GDPR is aimed primarily at EU-based businesses, it also applies to companies headquartered anywhere in the world that have stores in Europe or simply target sales to Europeans through the Internet, mobile apps or other remote commerce channels. The GDPR therefore has significant implications for many U.S. retailers.

Following adoption of the GDPR over two years ago, NRF engaged our retail company members and those of a counterpart EU-based retail trade association, EuroCommerce, in a multi-year transatlantic effort to develop the first common global retail approach to compliance with the GDPR. This collaborative work within the U.S. and European retail sectors culminated in the *GDPR Discussion Document for the Global Retail Industry,* a copy of which we have attached for your review. NRF and EuroCommerce *released* this discussion document in May and shared it with one of your witnesses today, Dr. Andrea Jelinek, Chair of the European Data Protection Board, as well as with European Data Protection Supervisor Giovanni Buttarelli and the data protection authorities (DPAs) in each of the current twenty-eight member nations of the EU.

Although our principal purpose in developing this GDPR white paper was to provide the basis for an on-going dialogue between the global retail industry and relevant stakeholders that would facilitate retail-specific approaches to GDPR compliance and enforcement, we believe this document has considerable importance for members of the Committee as you examine lessons learned from the GDPR. In the Committee's prior hearing, we noted that the Chairman and several other Committee members raised concerns that well-intended data privacy regulations could also have unintended consequences that either stifle technological innovation or lead to anti-competitive practices. In developing their compliance programs to meet the GDPR's requirements, retailers have discovered several elements of the GDPR that raise similar concerns. The attached GDPR discussion document takes great strides to illuminate specific areas where retailers' efforts to meet consumer expectations may be frustrated by the GDPR's approach to data regulation if DPAs' interpretations of the GDPR's provisions in the retail context are not carefully drawn.

In the attached discussion document, we have identified six critical areas of the GDPR that are highly relevant to the Committee's examination today, specifically: data erasure; data portability; the validity of prior consents; other legal bases for processing data, like legitimate interest; data breach notification; and automated decision-making, including profiling. We have found that well-meaning requirements in certain of these GDPR provisions may not align with existing consumer expectations, and we have strived to develop a retail approach to GDPR compliance to help minimize its unintended effects. We invite you to review this document and its discussion of areas where the intended purpose of the GDPR meets up with the reality of trying to practically implement a comprehensive global data privacy regulation in a way that will not upset customers' expectations with how they like to shop and receive personalized service from their favorite retailers.

Lessons Learned from the CCPA

In California, retailers face similar issues with the State's enacted data privacy law, but their concerns have been compounded by the fact that California spent little more than a legislative week trying to accomplish what took the EU nearly a decade to achieve with the GDPR. The underwhelming results are glaringly obvious, and businesses across industry sectors are facing a regulatory regime that, if it

takes effect as currently drafted, may create greater concerns for California consumers than benefits.

One of the more significant concerns we raised with the authors of the CCPA is that the law's anti-discrimination clause could lead to the decline of customer loyalty programs (*e.g.,* "club" discount cards, free merchandise, rewards, coupons, advanced release programs, exclusive experiences, etc.) offered by retailers and other businesses to California residents. The CCPA puts extraordinary pressure on these customer-favored programs by creating significant liability for businesses that provide rewards or other benefits, such as preferred service or pricing, to customers who sign up for these programs.

Under the CCPA, loyalty programs under which businesses provide preferred service or pricing to customers who opted in over customers who opt out of them are permitted only so long as the "value" of the personal information to the participating consumer used by the business is met by an equivalent value in discounts or benefits received by them. This is a legal equation fraught with such ambiguity that it invites an infinite array of "economic" opinions for state courts to weigh in potentially protracted, class action litigation. Personal data that may be "priceless" in the consumers' eyes would, if its value is defined by the consumer, never equate monetarily to a reasonable discount on a product. The potential for litigation over this most basic of retail transactions could lead some stores to shut down loyalty programs altogether as an untenable business litigation risk if they determine the potential costs of lawsuits outweigh the potential benefits to the business from providing the programs.

The CCPA raises other concerns that retailers will continue to address within the California legislature over the next fifteen months before the law is expected to take effect. For example, at the 11th hour, on the final day of the California session, the CCPA was amended by "clean-up" legislation to clarify the language of the bill. However, several of the so-called improvements were refinements to the exemptions in the bill that permit businesses with highly sensitive customer information to avoid the data privacy requirements that must be borne by other businesses handling the same or even less sensitive information. In some cases, there is no corresponding Federal law that would require the exempted sector from providing equivalent consumer data privacy protections. The CCPA's disparate treatment of businesses handling sensitive consumer data is one reason why Congress should move forward with comprehensive Federal legislation to establish a *uniform* set of requirements nationwide that applies evenly to all industry sectors handling similar sensitive personal information.

American consumers expect all businesses handling their sensitive information to do so responsibly, regardless of when and where that data is processed. By developing a data privacy law that does not pick regulatory winners and losers with the stroke of a pen before the stroke of midnight, Congress can ensure that Americans' privacy will be protected by Federal law regardless of which business is collecting, transmitting, storing or otherwise processing their sensitive personal information.

We look forward to working with the Committee to help members understand the deep flaws in the California regulation that hold the potential of significantly impacting e-commerce and exasperating consumers who could lose their preferred programs and benefits that they have come to expect. Congress would do well to avoid making the quickly-considered and problematic CCPA the model for Federal legislation.

As this Committee considers Federal data privacy legislation going forward, we urge you to continue to examine the lessons learned from the GDPR and CCPA, and to avoid the flaws in these and other foreign and state data regulations while preserving the more enlightened elements of the GDPR that would advance the U.S. approach to data privacy protection. We look forward to working with you and members of the Committee on Federal data privacy legislation that will provide a uniform and fair framework for consumers and businesses alike that respects and promotes consumer privacy.

Sincerely,

DAVID FRENCH,
Senior Vice President,
Government Relations.

cc: The Honorable Mitch McConnell
The Honorable Chuck Schumer
Members of the Senate Commerce Committee

Attachment

EUROCOMMERCE
NATIONAL RETAIL FEDERATION
25 May 2018

ANDREA JELINEK,
Chair, European Data Protection Board
Director, Osterreichische Datenschutzbehörde,
Wickenburggasse 8,
1080 Wien,
Austria.

Dear Chair Jelinek,

Following the adoption of the General Data Protection Regulation two years ago, EuroCommerce[1] and the National Retail Federation (NRF)[2] engaged our retail members operating in the EU and headquartered either in the EU or U.S. regarding implementation of critical elements of the GDPR. This transatlantic dialogue, which included a number of meetings of our associations and members with EU and U.S. officials in Brussels, has culminated in the *GDPR Discussion Document for the Global Retail Industry,* the first common global retail approach to compliance with the GDPR. Today, at this important moment for the GDPR, we are pleased to share with you this document.

Our principal purpose in developing this discussion document is to provide the basis for an on-going dialogue between the global retail industry and relevant GDPR stakeholders, including the Data Protection Authorities, the European Data Protection Supervisor and the European Commission, that facilitates retail-specific approaches to compliance and enforcement of the GDPR. It is intended as a living document, to evolve over time as our mutual understanding develops, as retailers' GDPR compliance practices are refined, and as enforcement of the GDPR takes shape. Our discussion document is also intended to help the global retail industry ensure their businesses are prepared for the implementation of the GDPR by its examination of key areas of common concern for retailers. Furthermore, we very much hope that our transatlantic cooperation can pave the way for a global approach that serves both the privacy concerns of citizens and the competitiveness of the global retail industry.

In light of the above, we would be delighted if you would accept our invitation to engage in an ongoing dialogue with us on the global retail industry's approach to GDPR compliance and enforcement. It is our firm intention to further cement this cooperation and, in parallel with the 40th International Conference of Data Protection & Privacy Commissioners to be held in Brussels this October, we plan to organize a number of meetings with national, EU and U.S. officials. We would greatly appreciate the opportunity to have a conversation with you then about our discussion document and, with that in mind, we will send you an official invitation in the coming weeks.

Yours sincerely,

CHRISTIAN VERSCHUEREN,
Director-General,
EuroCommerce.

MATTHEW R. SHAY,
President and CEO,
National Retail Federation.

Attachment: GDPR Discussion Document for the Global Retail Industry

---

[1] EuroCommerce is the principal European organization r presenting the retail and wholesale sector. It embraces national associations in 31 countries and 5.4 million companies, both leading multinational retailers and small family operations. Retail and wholesale provide a link between producers and 500 million European consumers over a billion times a day. It generates one in seven jobs, providing a varied career for 29 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognized European social partner for the retail and wholesale sector. *www.eurocommerce.eu*

[2] The National Retail Federation is the world's largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the largest private-sector employer in the United States, supporting one in four U.S. jobs—42 million working Americans. Contributing $2 6 trillion to annual GDP, retail is a daily barometer for the U.S. economy. *www.nrf.com*

ATTACHMENT

EUROCOMMERCE
NATIONAL RETAIL FEDERATION
May 17, 2018

RETAIL APPROACH TO IMPLEMENTING CRITICAL ELEMENTS OF THE GDPR

GDPR Discussion Document for the Global Retail Industry

The General Data Protection Regulation (GDPR)[1] sets out changes to almost every area of customer data processing. Retailers with storefronts, websites, mobile apps or other digital platforms through which they serve customers face new compliance standards, additional administrative burdens and liability for violations, as well more stringent enforcement and penalties.

Since the GDPR is both industry-neutral and channel-neutral, there are no sector-specific rules about the use of customers' personal data by retailers for various commercial purposes, whether online, on mobile apps, in physical store locations or omni-channel.

Customers, however, expect retailers to process personal data responsibly and seamlessly when serving them. To meet these expectations, retailers must find appropriate methods for GDPR compliance that further their customer relationships and do not frustrate them.

With the GDPR taking full effect, there are still many questions about how the GDPR applies to critical areas of retail operations, such as: using customer data for improved service or promotional opportunities, managing customer information databases and loyalty programs, collecting customer consents, and honoring customer rights to erase, or port to a competitor, a customer's personal data.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations. The purpose of this document is to share this experience with GDPR stakeholders, including data protection authorities (DPAs), to facilitate retail-specific approaches to compliance that will meet the requirements of the GDPR while ensuring that retailers can continue to provide customers with the personalization, omni-channel experiences and seamless retail operations that they expect.

1. Right to Erasure

- *Purpose of the rule*
  - This rule was proposed to address consumers' interests in removing their personal data from databases or web search inquiries if there is no compelling reason for businesses to keep that data.
  - In the retail context, the right to data erasure is subject to certain legal and operational limitations discussed below. DPAs should recognize these limitations in their enforcement of the GDPR and in guidelines on the scope of data subject to the right to erasure.
- *Retailers' interpretation*
  Maintaining records related to purchased goods.
- In compliance with the GDPR, retailers will offer customers choices in how to erase their personal data that is used for certain purposes (*e.g.,* targeted marketing), but due to the transactional nature of product purchase data, retailers must continue to maintain records of goods purchased by their customers.
- Erasing transactional data necessary to prevent fraud or reconcile card transactions, or to permit customers to return or exchange products, would frustrate customer expectations. It would also harm customers who could not later obtain a refund for unwanted products, or who could not exchange a product to maintain its value to the customer (*e.g.,* exchange clothing so it is the right size).
- To better serve customers and meet their expectations, retailers should not erase product purchase data that would weaken fraud protections or prevent payment reconciliation, product returns or product exchanges.
  - Purchase records are critical to serving customers who seek to make returns or exchanges, and to assisting them on purchasing or exchanging related items (*i.e.,* in the same style or series). For example, some records must be maintained for a period of time to reconcile payment card transactions, or to complete product returns or exchanges.

[1] Regulation (EU) 2016/679 adopted on 14 April 2016. The GDPR becomes enforceable on 25 May 2018 after a two-year implementation period concludes.

- Operationally, retailers need to retain data related to transactions for fraud detection or prevention, investigative or litigation purposes.

Compliance with legal obligations.

- Retailers appreciate that the GDPR takes into account that the right to erasure cannot apply to data that they are required by law to maintain as records of transactions. For example, some national laws require retailers to maintain transaction records for up to 10 years. Retailers cannot erase this data without violating these laws, and the GDPR should be interpreted and applied in a way that does not require violation of any national laws in order to comply with customer erasure requests.
- Similarly, retailers appreciate that the GDPR recognizes they cannot be responsible for ensuring data erasure when a government authority has legally requested or ordered it to provide the personal data as part of a government investigation or for other authorized purposes. Once the data is in the control of a government enforcement authority, agency or court, a retailer cannot ensure its erasure on systems outside of its control and may also be prohibited by the governmental authority from erasure of the data on its own system.

Customers' data on social media and review sites (third-party platforms).

- Customers who ask a retailer to remove personal data from the retailer's systems would not reasonably expect the retailer to follow the consumer online and erase data the consumer has voluntarily placed elsewhere.
- Third-party platforms, such as social media and consumer review websites, may post public comments from a consumer about a retailer, but the controller of that posted information is the platform operator, not the retailer.
- The GDPR's right to erasure therefore should not be construed as an affirmative obligation for retailers to follow customers' postings of personal data wherever that data appears online (*e.g.,* on social media or consumer review websites) to facilitate consumer erasure requests. Rather, third-party platforms that post public comments of consumers are the controllers of that information and have the principal obligation to erase personal data upon the consumer's request.

Compliance with customers' erasure requests.

- Successful retailers know that consumers expect them to innovate and deliver new content including consumer trends, top sellers, and the latest product or fashion developments. One way that retailers meet this customer expectation is by using and sharing aggregate or processed data that has been rendered non-personal data and is not subject to GDPR erasure requirements, including anonymized, aggregate customer data and data generated from personal information that does not identify a data subject.
- Some retailers may use deidentification tools to extract personal data from non-personal data sets that it retains for transactional, legal or other purposes. Consumers submitting erasure requests related to their personal information would not expect the retailer to erase information that no longer identifies them. Deidentification tools are just one of the methods available to retailers that enable compliance with erasure requests related to their personal data while preserving use of non-personal business data necessary for the retailer to maintain competitive operations.
- The right to erasure should not cover technical operations necessary to ensure the security of the relevant data, and should not apply to data captured in unstructured and unsearchable systems (*e.g.,* closed circuit security footage). Erasing data that leaves security systems vulnerable would be antithetical to data protection requirements to ensure customer data security, and the right to erasure should not extend that far. Additionally, the right to erasure should not require retailers to pull together data in unstructured systems to eliminate it; this would risk creating greater amounts of associated customer data which would be contrary to the data minimization principles in the GDPR.
- Businesses should be allowed to keep appropriate records of data erasure requests for evidencing accountability and demonstrating that they have complied with individuals' requests for data erasure.
- Retailers and customers should understand the above legal and operational limits on what data is appropriate to be erased under the GDPR's right of erasure and preserve the data necessary to fully meet customers' expectations.

2. Right to Data Portability

- *Purpose of the rule*
- This rule was proposed to protect consumers' interests in moving valuable account information (*e.g.,* utility usage, subscriber data) or media (*e.g.,* photos, documents) stored on one online service to a similar service provider.
- In the retail context, retailers and consumers reasonably expect the right to data portability to be applicable to data that is *not* transactional in nature (*i.e.,* data that must be maintained by the retailer) for the same reasons discussed above under the right to erasure. Additionally, retailers should recognize that the right to data portability covers *personal* data and does not extend to proprietary retail business information that, if required to be ported, could raise unfair competition concerns.
- DPAs should recognize these limitations on the scope of the right to data portability in its enforcement of the GDPR and in its guidelines on the proper scope of data that is subject to this right.
- *Retailers' interpretation*
- Retailers should continue to maintain the confidentiality of any data related to its customers (*e.g.,* information related to a loyalty plan) that is *neither* provided directly by the customer *nor* user-generated stored media (*e.g.,* photos created by the customer and uploaded to the retailers' system).
- Retailers appreciate that the right to data portability covers only *personal* data of a customer and not data that is derived from transactions or constitutes analytical inferences made by businesses from the behavior of their customers (*e.g.,* shopping habits/behavioral analytics).

Decoupling personal data (for porting purposes) from competitive or commercially-sensitive retail transactional data.

- When a customer's personal data and retail transactional data are associated, the right of portability should only extend to the personal data that can be decoupled from the competitive or commercially-sensitive transactional data, and that personal data should be ported without the portion constituting transactional data.
  - Retail business data should not fall within the scope of a customer's right to data portability, which was adopted as part of the GDPR to ensure that consumers could move their *personal* data to another business.
  - Requiring businesses to port competitive or commercially sensitive data to another competitor would go beyond the purposes for which the right was adopted.
  - If the right were to also cover associated transactional data along with consumers' personal data, it would raise significant competition concerns for retailers as it could reveal product sales strategy, trade secrets and other commercially sensitive business data to any competitor that receives the ported data.
  - Additionally, if such business data is included in this right, it is likely that unscrupulous competitors would abuse a customer's right to data portability by encouraging them to request the porting of competitive information from another retailer in return for receiving lower-priced products as compensation for requesting that transfer of business data.

Compliance with customers' data portability requests at time received.

- To practically comply with the GDPR, retailers must view the data portability request from customers as occurring at one moment in time and requiring porting of covered personal data that the retailer has in its possession at that time.
- The right to data portability should not create an ongoing requirement to periodically port to another party the customer's personal data accumulated since the time of the previous request. Such a requirement may not only be inconsistent with the customer's intent and future desires, but also would set up an unreasonable, perpetual porting obligation that would be too costly to maintain.

3. Consent

- *Purpose of the rule*

- The rules regarding consent were proposed to ensure that a customer ("data subject") has freely given his or her permission to a business ("controller") to process the customer's data for a specific purpose.
- The guidelines for consent adopted by the Article 29 Data Protection Working Party (WP29) state: "Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR. When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing." [2]
- Retailers have found that other lawful bases are appropriate grounds under the GDPR for most of the processing of customer data they can envisage, however, consent may be necessary for some processing or as an *additional* basis on which to ensure their processing of data is valid.
- *Retailers' interpretation*
- Established retailers have obtained the consent of data subjects to process their personal data for specific purposes for many years, and in some cases, several decades. As guidelines on consent are further developed by DPAs, retailers' views on how to implement consent in the retail context can be instructive to DPAs as they consider scenarios in which the GDPR requires consent.

Validity of prior consents.

- Retailers and consumers reasonably expect to rely upon prior consents obtained in compliance with existing laws before 25 May 2018 where a customer had *freely* given his or her permission to a retailer to process the customer's data for a *specific purpose.*
- Retailers support the WP29 guidelines' view that the GDPR's four consent conditions, coming into effect on 25 May 2018, are required for obtaining valid consent *on or after* that date. Because the GDPR's requirements cannot be retroactive, retailers call for clarification that the absence of providing its four customer notification requirements when a retailer validly obtained customer consent on a prior date *does not invalidate* the prior consent.
- Consumers expect, and retailers agree, that consents validly obtained under the 1995 Data Protection Directive should remain valid and *should not require* the customer to resubmit the same consent. (Similarly, as noted below, consents validly obtained under the e-Privacy Directive *should remain valid* pending adoption of new rules in the EU's forthcoming e-Privacy Regulation.)
- Requiring companies to re-obtain consent where it was validly obtained before for the same purpose is also counterproductive because it places enormous burdens on consumers, not just businesses.
  - For example, if re-obtaining consents in these situations is required for retailers, customers could face hundreds of new e-mails, phone calls or mailed notices asking for their reconfirmation of prior consents for the same purposes.
  - Additionally, customer re-consent in the physical retail space could add unnecessary time to each transaction—inconveniencing consumers who prefer to shop in stores instead of online.
  - These consequences run counter to: (i) sound public policy that seeks to minimize the number of solicitations consumers receive; and (ii) an enhanced, customer experience that is intended to be more pleasant, streamlined and efficient for consumers.
  - For these reasons, valid prior consents should be relied upon by retailers and their customers, and re-obtaining consent for the same data processing purposes should not be required.

Application of GDPR to valid consent under e-Privacy Directive.

- A related issue regarding the validity of customer consents previously obtained under existing law is raised by the unclear text of the final paragraph of section 1 of the WP29's guidelines on consent with respect to the application of the GDPR consent conditions to situations falling within the scope of the e-Privacy Directive (2002/58/EC). The text in this paragraph states that the GDPR consent conditions are "preconditions for lawful processing," but are "not considered

[2] See *Guidelines on consent under Regulation 2016/679,* adopted on 28 November 2017, as last revised and adopted on 10 April 2018 (*http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051*).

to be an 'additional obligation'" prohibited by Article 95 of the GDPR. Retailers find this language confusing in light of the continued operation of the e-Privacy Directive pending the adoption of the forthcoming e-Privacy Regulation that will replace it.

- The WP29's consent guidelines could be interpreted to require businesses to apply the GDPR consent conditions *retroactively* to previously obtained customer consents that presently fall within the scope of the e-Privacy Directive. In our view, any new conditions for consent not presently required by the e-Privacy Directive would amount to additional obligations that are prohibited by Article 95. Retailers have therefore called for clarification from DPAs that additional steps are not required to validly obtain consent under the currently effective e-Privacy Directive, and that the GDPR does not automatically invalidate the consents previously validly obtained under the e-Privacy Directive prior to adoption of the forthcoming e-Privacy Regulation.
- Retailers have a practical concern with the application of the GDPR consent conditions to situations falling within the scope of the current e-Privacy Directive and that will again fall within the scope of the forthcoming e-Privacy Regulation. Retail businesses anticipate that certain data processing practices will need to be updated to comply with the new e-Privacy Regulation once it is adopted, and they are concerned that the guidelines require business practices to be updated twice: first, to add GDPR consent conditions to obtain valid consent under the e-Privacy Directive prior to adoption of the e-Privacy Regulation; and second, upon adoption of the e-Privacy Regulation (particularly if additional legal bases or conditions for processing are adopted).
- Requirements to serially change business practices over a short period of time to obtain valid consent for processing—through adoption of new consent practices for a short interim period before adopting different, long-term compliance practices—will needlessly complicate business efforts to comply with both the GDPR and e-Privacy Regulation. Retailers believe it will also create additional confusion for their customers who may, as a result, receive multiple solicitations seeking their consent for the same process within a short time (when the e-Privacy Directive is later replaced by the e-Privacy Regulation).
- Retailers would appreciate further efforts by DPAs to clarify the interpretation of the GDPR for compliance purposes to ensure that retail businesses validly obtaining consents under the current e-Privacy Directive—using practices for obtaining such consents as currently implemented—may continue to rely upon the validity of those consents at least until the establishment of new consent requirements upon the adoption of the forthcoming e-Privacy Regulation, provided that in the interim the consented-to processing activities remain unchanged and that reasonable withdrawal of prior consents remains available.
- Finally, retailers acknowledge that the relationship between the GDPR and the e-Privacy Directive has not yet been fully harmonized. This follows from GDPR Recital 173 which states that the e-Privacy Directive must be reviewed *and amended* for purposes of ensuring the e-Privacy Directive's consistency with, and clarifying its relationship to, the GDPR. Until businesses receive the clarity and consistency called for by the GDPR, we respectfully ask DPAs to defer their inquiries into business practices that are currently in compliance with the e-Privacy Directive.

Retail considerations for consents obtained in compliance with GDPR.

- Where relying on existing consents is not possible and consents need to be refreshed, a retailer's notice or request to consumers to update their consent should not be considered a direct marketing communication.
- With respect to consents obtained for multiple store brands under the control of one retail company, a global consent process may be used so that the retailer is not required to obtain separate consents for the same process for each brand under its control, provided that the customer is informed of all store brands to which she is giving her consent.
- If crafted in a way that clearly does not limit other methods to comply, retailers would evaluate the efficacy of a single, comprehensive process to collect consent, applicable to the retail context, that is compliant with the consent requirements of the GDPR.

Relying on consent obtained by other controllers.

- With respect to consents required to be obtained by a retailer from customers using a retail store's mobile app, retailers should be able to rely upon the stand-

ardized mechanism in the mobile app platform (*e.g.,* Apple's App Store, Google's Play Store) to demonstrate that the consent to download and install the app, and to activate certain app features (*e.g.,* location tracking), was informed and freely given for the specific purpose of using the app.

- Retailers cannot alter the app market's process by which a customer consents to download and install a mobile app on a smart phone, and must therefore rely on the app market's or smart phone's standard consent process as evidence that the customer validly consented to download, install and activate the mobile app.

4. Other Legal Bases for Retail Processing of Customer Data: Legitimate Interest and Contractual Necessity

- *Purpose of the rule*
- The GDPR's six legal bases for processing allow flexibility in how companies may use personal data for their own business purposes while ensuring individuals' rights are respected.
- As noted in section 3 above, there are five other legal bases for processing data under the GDPR that retailers may rely upon other than a customer's consent. Retailers may therefore determine that they already have a legitimate interest or contractual necessity, among other legal bases, to process customer data for common retail purposes.
- *Retailers' interpretation*

Ensuring seamless shopping experience for customers.

- Customers expect retailers to process their data when it is a necessary component of the underlying retail shopping experience. Consumers do not expect retailers to interrupt their shopping, or serially notify them, simply to obtain their affirmative consent for every aspect of the retailer-customer interaction that requires some type of data processing.
  - Such a practice would be very disruptive to the customer's shopping experience, whether online, mobile or in-store, and customers would likely reject it as annoying and unnecessarily burdensome on them.
- To meet customers' expectations of a seamless shopping experience based on responsible data use, retailers may rely upon other legal grounds to process customer data, such as in cases where they can demonstrate a legitimate interest or contractual necessity to process customer data.
  - The examples are as varied as the number of consumers and retailers, but customers understand that retailers' collection, use and retention of personal information is part of an individualized retailer-consumer experience.
  - Therefore, under the GDPR, absent consent, retailers would ensure having a legitimate interest in, or a contractually necessary basis for, processing customer data and that the purpose for the data collection, the duration for which it is retained and other elements that constitute lawful processing are met in a manner that is most appropriate for consumers in the retail context.

Loyalty programs and common in-store transactions.

- A common retailer-customer experience where neither the consumer nor the retailer would expect serial consent solicitations to be required is for promotions or discounts received from retail loyalty programs in which the consumer enrolls. Retailers may justify such data processing on other legal bases under the GDPR. Loyalty programs may be distinguished from marketing or profiling communications that otherwise might require consent.
- Additionally, many common in-store transactions, where requesting consent could be disruptive to the shopping experience, may be lawfully grounded on the bases of legitimate interest or contractual necessity.

Other retailer considerations for lawful processing.

- If crafted in a manner that would not limit other ways to comply, retailers would evaluate the use of a uniform approach to what constitutes "legitimate interest" or "contractual necessity" in the retail context.
- Retailers also call for a coherent implementation of the legitimate interest and contractual necessity grounds to avoid conflicting regulatory requirements for processed data if these legal bases are not adopted as lawful grounds for processing data under the EU's forthcoming e-Privacy Regulation.

5. Data Breach Notice

- *Purpose of the rule*
- This rule was proposed to create incentives for businesses to improve their overall data security practices and to give regulators greater oversight over data security risks and breaches.
- *Retailers' interpretation*
- Retailers support breach notification for *all* businesses suffering breaches of customer data.

Breaches suffered by co-controllers of data.

- Retailers would appreciate a recognition by DPAs that certain breached service providers are data controllers in their own right and effectively operate as co-controllers of the retail customer's payment card data. As controllers themselves, these service providers should make the required notices to regulators and individuals of their own breaches.
  - Some data processing by third parties to retailers, such as card payments services, involves massive amounts of cardholder payment processing where relatively few payments services providers and branded card networks collect and route payments for millions of retailers.[3]
  - When breaches are incurred by these and similar one-to-many service providers, individual retailers are neither in position to know the circumstances of the breach nor determine if it is likely to create a high risk to individuals' rights.
  - Furthermore, placing the notice requirement exclusively on the unbreached retailers alone in these multi-party scenarios could trigger the delivery of thousands of separate breach notices to regulators for the single breach. If notice to affected individuals is also required, customers could conceivably receive dozens of notices about the same service provider's breach, with the content of each notice likely being different (due to incomplete information provided by the breached entity to thousands of unbreached retailers making notice).
- Recognizing such service providers as data controllers in these and similar one-to-many service provider scenarios would prevent the potential massive over-notification of regulators and affected individuals for a single breach, and the resulting consumer confusion created by this type of data breach notice rule where such recognition is not made by DPAs.

Breach notice time limits.

- Retailers support reasonable and practical time limits to make required notices, where the clock starts running only when the party with the notice obligation first learns of the breach. (This interpretation would enable data controllers to make timely notice where a data processor unreasonably delays notification of its own breach to the controller.)
- Retailers support the interpretation that a notification obligation is triggered when a business has actual knowledge or confirmation of a breach, not merely a suspicion. Notifying unnecessarily in circumstances with no actionable information, and where no risk of harm to individuals has been established, could potentially overwhelm both individuals and regulators.

Breach notice template.

- To ensure uniform enforcement, retailers would support a voluntary template that indicates information to be included in a breach notice.

---

[3] Consistent with the WP29's previous opinion on controllers (*see:* WP29 Opinion 1/2010 on the concepts of "controller" and "processor" adopted on 16 February 2010), these payment service providers (PSPs) are data controllers, in their own right, because: (i) PSPs have complete discretion in how to process card payments so long as they complete a card transaction for a retailer in a timely manner; (ii) nearly all retailers have no contractual authority to actively monitor the level of service (other than completion of a transaction) or audit the card data processing by PSPs; and (iii) data subjects' expectations when offering a card for payment is that they are initiating a financial transaction that sends the card information to their bank for authorization and they do not expect the retailer itself to complete this transaction unless it is the issuer of the card they use.

6. Automated Decision-Making, including Profiling

- *Purpose of the rule*
- This rule was proposed to ensure that individuals are not subject to a decision affecting them uniquely that is based *solely* on automated processing and that any such decision will be reviewed if it produces adverse legal effects or other similarly significant effects.
- *Retailers' interpretation*
- Retailers and consumers understand that customized advertising and offerings rely on automated tools and automated decision making.
- Retailers support the interpretation in the WP29 guidelines on automated decision-making that, in many cases, customized advertising does not typically have a significant effect on individuals. For this reason, most online customized advertising does not require consent, which is consistent with consumers expectations as well.
- Retailers should evaluate whether and when automated decision-making might produce unintended discriminatory consequences, especially regarding pricing, that may require informed consent.
- Retailers appreciate confirmation by DPAs that the scope of the profiling provision is limited to actual decisions, which relate to a specific individual, rather than any data analytics used, for instance, to improve customer services without making a decision in relation to a specific individual.

Inquiries about this GDPR Discussion Document may be directed to:

JOANNA LOPATOWSKA,
Adviser, Consumer Policy & Digital,
EuroCommerce.
lopatowska@eurocommerce.eu

PAUL MARTINO,
Vice President, Senior Policy Counsel,
National Retail Federation.
martinop@nrf.com

About EuroCommerce

EuroCommerce is the principal European organization representing the retail and wholesale sector. It embraces national associations in 31 countries and 5.4 million companies, both leading multinational retailers such as Carrefour, Ikea, Metro and Tesco, and many small family operations. Retail and wholesale provide a link between producers and 500 million European consumers over a billion times a day. It generates one in seven jobs, providing a varied career for 29 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognized European social partner for the retail and wholesale sector. *www.eurocommerce.eu*

About NRF

The National Retail Federation is the world's largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the largest private-sector employer in the United States, supporting one in four U.S. jobs—42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the U.S. economy. *www.nrf.com*

PUBLIC KNOWLEDGE
Washington, DC, October 10, 2018

Hon. JOHN THUNE,
Chairman,
Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Hon. BILL NELSON,
Ranking Member,
Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

On behalf of Public Knowledge, a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works, we submit this statement for the record for the Senate Committee on Commerce, Science, and Transportation hearing on "Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act."

It is no longer possible to participate in society without providing data to third parties that may, in and of themselves be personal, or that, when combined with other data and analyzed, may reveal intimate information. The consequences of this data acquisition, analysis, use, and sharing can be profound for individuals' lives. For example, data have been used to show certain job postings only to men [1] and to exclude African-Americans from seeing certain housing advertisements.[2] In the 2016 election, Russian agents were able to use data to target advertisements to African-Americans to urge them not to vote.[3] Data exploitation enables "unequal consumer treatment, financial fraud, identity theft, manipulative marketing, and discrimination." [4] Against this backdrop, the Committee's consideration of appropriate safeguards for consumer data privacy could not be timelier.

We are pleased that the Committee appears to be taking seriously the privacy concerns facing consumers in the digital age and welcome the opportunity to submit the following principles that must be reflected in any comprehensive privacy legislation.

Scope

It is widely agreed that any comprehensive privacy legislation must cover both ISPs and edge providers.[5] However, comprehensive legislation must recognize the disparate ways that different entities use, collect, and, indeed, require personal data, and it must treat different entities differently. For example, an ISP requires an individual's physical address in order to deliver Internet service; Facebook or Twitter does not need an individual's physical address in order for their service to function. Similarly, by virtue of owning the pipes, ISPs are able to collect significantly more data about individuals than edge providers can; ISPs can view the entirety of an individual's Internet activity; they also have information about whether the individual pays his or her cable bill on time. An edge provider—even one that makes prolific use of tracking pixels on third party websites—has only a fraction of an ISP's insights on a given consumer. This means that if legislation allows for exceptions for data used for legitimate business purposes,[6] it is appropriate to tailor what data are exempted for different entities (rather than, say, exempting all address information, because ISPs need it). All entities in the ecosystem should, of course, have the same obligations to protect and adhere to notice and consent requirements [7] for the data they do collect.

Additionally, the Federal Communications Commission (FCC) is the expert agency with oversight over ISPs and all communications networks; whereas, the Federal Trade Commission (FTC) is the expert agency with oversight over edge providers. There is no reason to disrupt this division of labor. Rather, comprehensive privacy legislation should build on the respective agencies' years of experience with and knowledge of the entities they oversee.

Any comprehensive privacy legislation must also reflect the ways in which data are actually used. Many edge providers do not sell data.[8] Rather, they leverage data to sell advertisements. An advertiser approaches an edge provider with an audience it would like to reach (say, suburban women with children, between the ages of 30 and 45, who like the color blue), and the edge provider uses the data it maintains to match the ad to the desired audience.[9] The fact that the data do not change hands is immaterial for consumers' experiences. Consumers are aware that companies profit off of their personal information even if that information is not sold *qua* sold. Moreover, this sort of ad targeting enables the types of nefarious advertising

---

[1] *See* UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).

[2] Julia Angwin, Ariana Tobin, and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users By Race,* PROPUBLICA, Nov. 21, 2017.

[3] Natasha Singer, *Just Don't Call It Privacy,* NY TIMES, Sept. 23, 2018, *https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.*

[4] *Id.*

[5] *E.g.* INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018); U.S. CHAMBER, PRIVACY PRINCIPLES (2018).

[6] For further discussion, *see* p. 5 *infra.*

[7] *See* pp. 3–5 *infra.*

[8] *E.g.* Kurt Wagner, *This is how Facebook uses your data for ad targeting,* RECODE, Apr. 11, 2018, *https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg.*

[9] *Id.* Some edge providers are also set up to find look-alike audiences with similar traits a pre-populated list an advertiser provides. Some also permit an advertiser to target particular individuals. UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).

practices described above where women and older workers are not shown particular job postings and racial minorities are denied access to housing ads.[10]

Even where data are not sold, data may change hands in other ways. For example, researchers and app developers frequently have access to consumer data held by edge providers. At the end of March, we learned that one such app developer, Aleksandr Kogan, funneled personal information about at least 87 million Facebook users to Cambridge Analytica, a firm that purported to engage in "psychographics" to influence voters on behalf of the Trump campaign. Gallingly, as was Facebook's practice for all apps at that time, when users connected Kogan's app to their Facebook accounts, the app scooped up not only the users' personal information, but also their friends' information—without any notice to the friends or opportunity for the friends to consent.

And, of course, data breaches continue to proliferate. Just between the time the Facebook/Cambridge Analytica news broke in March 2018 and this Committee's hearing with Mark Zuckerberg in April 2018, consumers learned of data breaches at Orbitz, Under Armour, Lord and Taylor, Saks Fifth Avenue, Saks Off Fifth, Panera Bread, Sears Holding Corp., and Delta Airlines. IBM reports that the average cost of a data breach reached $3.86 million in 2017.[11]

Given the myriad ways that personal data are collected, used, and shared, any comprehensive privacy legislation must cover the full lifecycle of consumer data, including collection, use, retention, sharing, and selling of consumer data.[12]

Sensitive/Non-Sensitive Distinction

The sensitive/non-sensitive distinction, which provides heightened protections to so-called sensitive information, like first and last name, social security numbers, bank account numbers, etc., and lesser protections to other information is increasingly illogical in today's world and should be eschewed in any comprehensive privacy legislation. Not only can so-called non-sensitive information be aggregated to reveal sensitive information, but if Facebook/Cambridge Analytica taught us anything, it is that "non-sensitive" information, like social media "likes," is useful for marketing and advertising, and also, if Cambridge Analytica (and, for that matter, the Obama campaign)[13] is to be believed, for highly sensitive activities like influencing individuals in the voting booth.

Notice and Consent

Until the digital age, individual ownership and control of one's own personal information was the basis for privacy law in the United States.[14] We should return to this principle. While we cannot avoid sharing information with some third parties, we can have greater control over that information. At a minimum, consumers should have a right to know (a) what information is being collected and retained about them; (b) how long that information is being retained; (c) for what purposes that information is being retained; (d) whether the retained information is identifiable, pseudo-anonymized, or anonymized; (e) whether and how that information is being used; (f) with whom that information is being shared; (g) for what purposes that information is being shared; (h) under what rubric that information is being shared (for free, in exchange for compensation, subject to a probable cause warrant, etc.); and (i) whether such information is being protected with industry-recognized best security practices.[15]

---

[10] *See supra* notes 1–3.

[11] IBM, COST OF A DATA BREACH STUDY (2018).

[12] In fact, even the Internet Association shares this view, writing in their own privacy principles that, "Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared. . .". INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018).

[13] Sasha Issenberg, *How Obama's Team Used Big Data to Rally Voters,* MIT TECH. REV., Dec. 19, 2012, *https://www.technologyreview.com/s/509026/how-obamas-team-used-big-data-to-rally-voters/*.

[14] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19–20 (Public Knowledge, 2017).

[15] Consumer advocates are not alone in calling for meaningful notice. Both the Internet Association and The Software Alliance also call for notice. INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018) ("Transparency. Individuals should have the ability to know if and how personal information they provide is used and shared, who it's being shared with, and why it's being shared."); THE SOFTWARE ALLIANCE, BSA PRIVACY PRINCIPLES (2018) ("Transparency[.] Organizations should provide clear and accessible explanations of their practices for handling personal data, including the categories of personal data they collect, the type of third parties with whom they share data, and the description of processes the organization maintains to review, request changes to, request a copy of, or delete personal data.")

It is imperative that this notice be meaningful and effective, which means that it cannot be buried in the fine print of a lengthy privacy policy or terms of service agreement. Consumers and companies know that consumers do not typically read privacy policies or terms of service agreements. Indeed, researchers at Carnegie Mellon estimate that it would take seventy-six work days for an individual to read all of the privacy policies she encounters in a year.[16] Companies take advantage of this common knowledge to bury provisions that they know consumers are unlikely to agree to in the fine print of these agreements. While courts have found these agreements to be binding contract, there is no reason that Congress cannot undo this presumption and insist that notice be provided in a way that consumers can quickly read and understand.

Moreover, notice alone is insufficient. Consumers must also have meaningful opportunities to freely and affirmatively consent to data collection, retention, use, and sharing. And, that consent should be as granular as possible. For example, a user should be able to consent for her data to be used for research purposes, but not for targeted advertising—or vice-versa. As with notice, the consent must be real rather than implied in the fine print of a terms of service. Consumers must also have the ability to withdraw their consent if they no longer wish for a company to use and retain their personal data, and they should be able to port their data in a machine-readable format to another service, if they so desire.[17] In addition, service should not be contingent on the sharing of data that is not necessary to render the service.[18]

The General Data Protection Regulation (GDPR), which went into effect in Europe in May, requires some kinds of granular notice and consent, so companies already have had to figure out how to offer their users opportunities for meaningful consent. There is no reason for them not to offer the same opportunities for meaningful notice and consent in the United States. Moreover, Europe will prove an interesting testing ground, and the United States can learn from the notice and consent practices that are most effective in Europe.

While it may be appropriate to allow implied consent for data that are integral to render the requested service (such as a mailing address and credit card number if one wishes to order a product on Amazon),[19] these exceptions must be narrowly drawn. Allowing companies to collect, retain, use, and share, all personal data they deem "necessary for the basic operation of the business,"[20] as the Internet Association suggests, may permit any advertising-supported platform to collect, retain, use, and share any and all consumer data. After all, if the basic operation of the business is to deliver advertising, increased data makes ad delivery more precise and efficient. Congress must ensure that any exceptions are appropriately narrowly tailored to avoid such an absurd result that would eclipse the rule.

Security

Organizations that are stewards of our personal information should be expected to adhere to recognized best practices to secure the information. This is particularly true when an individual cannot avoid sharing the information without foregoing critical services or declining to participate in modern society.

---

[16] Alexis C. Madrigal, *Reading the Privacy Policies you Encounter in a Year Would Take 76 Work Days,* THE ATLANTIC, Mar. 1, 2012, *https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/*.

[17] This is another recommendation where advocates and industry align. *See* THE SOFTWARE ALLIANCE, BSA PRIVACY PRINCIPLES (2018).

[18] While it may be appropriate for a non-essential service like Facebook to charge users a fee in lieu of selling their data, *see* Alex Johnson and Erik Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says,* NBC NEWS, Apr. 5, 2018, *https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151,* such an approach is unacceptable for services that are integral for participation in society. Individuals should be able to access health care, education, housing, and other essential services without compromising their personal information or having to pay extra for their fundamental right to privacy.

[19] The alternative approach, which GDPR takes, would be to allow companies to refuse service when a consumer neglects to consent to the collection and use of information required to render the requested service.

[20] INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018).

Relatedly, organizations should be required to adhere to privacy by design and by default[21] and to practice data minimization.[22] The presumption should be that only data necessary for the requested transaction will be retained, absent explicit consumer consent. Organizations should be encouraged to employ encryption, pseudo-anonymization, and anonymization to protect consumers' private information, and security mechanisms should be regularly evaluated. Importantly, these evaluations must be publicly reported to enable transparency and accountability. In addition, the government should act as convener of any multi-stakeholder process to develop privacy and/or security standards. Facebook/Cambridge Analytica, as well as the cascade of recent data breaches, has demonstrated that industry cannot be trusted to police itself.

Furthermore, entities that experience a data breach should be required to notify consumers of the breach shortly after it occurs without any required showing of "harm." Since the days of Justice Brandeis, individual ownership and control of one's own personal information has been the basis for privacy law in the United States.[23] There is increasing consensus that this principle should endure in the digital age.[24] With this principle in mind, the harm occurs when personal information is acquired or accessed in a way that is unanticipated or unauthorized by the individual to whom the information pertains. As a result, individuals should be notified of a data breach upon discovery of the breach. This will allow individuals to take prophylactic measures to protect themselves from further injury.

Furthermore, the tangible harms one may be exposed to when her data are breached or shared in an unauthorized way extend far beyond the boundaries of legally-cognizable harm. For example, a data breach may expose information that could be embarrassing or that could re-endanger a domestic violence victim. Tangible harms may also come in the form of Cambridge Analytica-style "psychographics." And, the tangible injuries individuals may experience after a data breach may change as technology changes. It is impossible to foresee and legislate for all possible harms.

Moreover, codifying the harm standard simply allows the entity that has already failed to sufficiently protect sensitive personal information to determine, in its sole discretion—when it has every financial incentive to keep a data breach secret—whether or not consumers have been or will be harmed and thus whether or not consumers should be informed of the breach.

The occurrence standard is entirely workable. In fact, the GDPR adopts an occurrence standard for breach notification. Companies that notify their European customers of a breach when it occurs but that fail to notify their U.S. customers until there is demonstrable harm from the breach are likely to face backlash from their U.S. customers.

Meaningful Recourse

When there is unauthorized access to personal information, individuals must be made whole to the greatest extent possible. There are two major barriers to this. The first is the Federal Arbitration Act, which requires courts to honor the forced arbitration clauses in contracts, including forced arbitration clauses buried in the fine print of terms of service agreements. Forced arbitration clauses require consumers to settle any dispute they have with a company by arbitration rather than having their day in court—and often consumers do not even know an arbitration clause is in their contract until they go to sue. This presents three problems: (1) Arbitrators are often more sympathetic to large companies, who are repeat players in the arbitration system, than most juries would be. (2) Arbitration creates no legal precedent. (3) Frequently, it is not cost-effective for an individual to bring a claim against a large company by herself. The damages she could win likely would not exceed her legal costs. But, when customers can band together in a class action lawsuit, it becomes much more feasible to bring a case against a large company en-

---

[21] Again here there are synergies with industry recommendations. *See id.;* U.S. CHAMBER, PRIVACY PRINCIPLES (2018).

[22] *See The Code of Fair Information Practice Principles,* U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973).

[23] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19–20 (Public Knowledge, 2017).

[24] *E.g. Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on the Judiciary & the S. Comm. on Commerce, Sci., & Transp.,* 115th Cong. (2018) (Statement of Mark Zuckerberg, CEO, Facebook); *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Commerce,* 115th Cong. (2018) (Statement of Mark Zuckerberg, CEO, Facebook); Scott McDonald, President & CEO, ARF, Townhall at ARF Townhall on Research Ethics Partnered with GreenBook (Apr. 26, 2018).

gaged in bad behavior. Forced arbitration clauses preclude class action. Congress should explicitly exempt cases addressing the failure to protect personal information from the Federal Arbitration Act to make sure consumers can have their day in court when their information is misused and their trust abused.

The second major barrier to meaningful recourse is the difficulty calculating the damages associated with unauthorized access to personal information. While one may be able to quantify her damages when her credit card information is breached or her identity is stolen, it is much harder to do so in a situation like Facebook/Cambridge Analytica. It is difficult to put a dollar amount on having one's privacy preferences ignored or her personal information revealed to third parties without her knowledge or consent. We instinctively know that there is harm in having one's personal data used for "psychographics" to influence her behavior in the voting booth, but that harm is difficult to quantify. Congress already uses liquidated damages in other situations when the damage is real, but hard to quantify. In fact, liquidated damages are already used to address other privacy harms. For example, the Cable Privacy Act provides for liquidated damages when cable companies impermissibly share or retain personally identifiable information.[25]

While the FTC can step in when companies engage in unfair and deceptive practices, the FTC is likely to only intervene in the most egregious cases. Moreover, the FTC can only extract damages from companies once they have violated users' privacy once, entered into a consent decree with the Agency, and then violated the consent decree. That means a lot of consumers must have their personal information abused before a company is held to account. Moreover, when the FTC is involved, any damages go to the government, not to making individuals whole.

We are not recommending that the FTC be taken out of the business of protecting consumers in the digital age—in fact, as described below, we believe that any comprehensive privacy legislation must strengthen the FTC (or another enforcement agency) and provide it with rulemaking authority. We are merely suggesting that consumers should also have the opportunity to protect themselves. Allowing private, class action lawsuits for liquidated damages when companies fail to safeguard private information will create the necessary incentives for companies to take appropriate precautions to protect the information they have been entrusted with. Companies, after all, understand the technology and the risks and are in the best position to develop safeguards to protect consumers.

Strong Oversight Agency with Rulemaking Authority

Any comprehensive privacy law must also be enforced by a strong oversight agency with sufficient resources and rulemaking authority. Former FTC Commissioners and staff have lamented that the FTC is not sufficiently resourced to protect consumer privacy in the digital age.[26] Since 2010, FTC funding has fallen five percent.[27] The Commission is unable pay the competitive salaries necessary to lure technologists from the private sector and as a result suffers from a dearth of technical expertise.[28] If the FTC is to be a sufficient cop on the beat protecting consumer privacy, it simply must have the resources and technical expertise commensurate with the task.[29]

Furthermore, the FTC, at present, only has the authority to respond to a privacy violation after it has occurred—in fact, the FTC is only able to impose penalties after a privacy violation has happened, the errant company has entered into a consent decree with the FTC and violated the consent decree, and the FTC has gone to court to sue the errant company. This rubric is insufficient to protect consumer privacy in the digital age. Rather, the FTC must have the ability to prevent privacy violations before they occur. The Commission needs rulemaking authority to create

---

[25] 47 U.S.C. § 551(f)(2)(A) (2001).

[26] *E.g.* Terrell McSweeny, Former FTC Commissioner, Open Tech. Inst., Facebook After Cambridge Analytica: What Should We Do Now? (Apr. 5, 2018); Tony Romm, *The agency in charge of policing Facebook and Google is 103 years old. Can it modernize?,* WASH. POST, May 4, 2018, *https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/*.

[27] David McCabe, *Mergers are spiking, but antitrust cop funding isn't,* AXIOS, May 7, 2018, *https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486-4a08-ab57-d3535ae43b52.html.*

[28] Tony Romm, *The agency in charge of policing Facebook and Google is 103 years old. Can it modernize?,* WASH. POST, May 4, 2018, *https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/; see also* Terrell McSweeny, Former FTC Commissioner, Open Tech. Inst., Facebook After Cambridge Analytica: What Should We Do Now? (Apr. 5, 2018).

[29] *See* Dylan Gilbert, *The FTC Must Be Empowered to Protect Our Privacy,* PUBLIC KNOWLEDGE, June 18, 2018, *https://www.publicknowledge.org/news-blog/blogs/the-ftc-must-be-empowered-to-protect-our-privacy.*

ex ante rules of the road that provide predictability for companies and sufficient privacy protections for consumers.[30]

Rulemaking authority is particularly important because of the pace at which Congress legislates. The legislative process is, in fact, designed to be slow.[31] The Telecommunications Act was last updated in 1996.[32] The Electronic Communications Privacy Act was authored in 1986—before the advent of the World Wide Web—and has not meaningfully been updated since.[33] Google is currently rolling out an update to Gmail.[34] Apple released its latest operating system for its iPhones and iPads on September 17, 2018.[35] Congress cannot hope to keep pace with the rate at which the technology industry innovates. Therefore, it is incumbent upon Congress to empower an oversight agency, which can move more nimbly than Congress can, with rulemaking authority so that the agency can update the rules to keep up with technological changes, as well as with new harms that may arise as technology develops.

Existing Laws

We encourage Congress to enact legislation that is compatible with existing Federal sector-specific privacy laws in communications, health care, finance, and other sectors, as well as with state and local privacy laws.

Moreover, while the Federal government should set minimum standards of protection for all Americans, states have been in the vanguard of privacy protection and are much-needed cops on the beat. Even if Congress were to dramatically expand the resources available to Federal privacy agencies, the Federal government could not hope to provide adequate protection to consumers on its own. For example, the FTC is unlikely to get involved in a data breach affecting consumers in just one state. In fact, Massachusetts Assistant Attorney General Sara Cable recently testified that less than one percent of data breaches in Massachusetts affect more than 5,000 people.[36] It is difficult to imagine Federal resources being used to investigate a data breach of this size, but a state like Massachusetts might choose to get involved. In fact, Massachusetts is likely to set a breach notification standard that is more appropriate for its state than the Federal government might set. For this reason, the states, as laboratories of democracy, should be empowered to innovate and provide greater privacy protections to their residents.

Conclusion

We appreciate the opportunity to submit this statement for the record and stand ready to assist the Committee as it continues to consider consumer privacy. If you have any questions or would like more information, please do not hesitate to reach out to me at abohm@publicknowledge.org.

Thank you,

ALLISON S. BOHM,
Policy Counsel,
Public Knowledge.

CC. Members of the Senate Committee on Commerce, Science, and Transportation

---

PREPARED STATEMENT OF THE AMERICAN BANKERS ASSOCIATION

Chairman Thune, Ranking Member Nelson and members of the Committee, the American Bankers Association ("ABA") appreciates the opportunity to provide its views on consumer data protection and privacy. The ABA is the voice of the Nation's $17 trillion banking industry, which is comprised of small, midsized, regional and large banks. Together, these institutions employ more than 2 million people, safeguard $13 trillion in deposits and extend more than $9.5 trillion in loans. Our mem-

---

[30] *See id.*

[31] Robert Pear, *The Nation; Gridlock, the Way It Used to Be,* NY TIMES, Oct. 9, 1994, *https://www.nytimes.com/1994/10/09/weekinreview/the-nation-gridlock-the-way-it-used-to-be.html.*

[32] *Telecommunications Act of 1996,* FCC, June 20, 2013, *https://www.fcc.gov/general/telecommunications-act-1996.*

[33] *Modernizing the Electronic Communications Privacy Act (ECPA),* ACLU, *https://www.aclu.org/issues/privacy-technology/internet-privacy/modernizing-electronic-communications-privacy-act-ecpa* (last visited Sept. 25, 2018).

[34] *What's new in Gmail,* GOOGLE, *https://support.google.com/a/answer/7684334?hl=en* (last visited Sept. 25, 2018).

[35] Matt Swinder, *iOS 12: new features and the iOS 12.1 release date,* TECHRADAR, Sept. 24, 2018, *https://www.techradar.com/news/ios-12.*

[36] *Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime Before H. Comm. on Financial Services, Subcomm. on Financial Institutions and Consumer Credit,* 115th Cong. (2018) (statement of Sara Cable, Assistant Attorney General, Massachusetts).

bers have a substantial interest in consumer data protection and privacy and we respectfully request that this statement be included as a part of the record for today's hearing.

A. Banks and Financial Institutions Already Are Subject to Extensive Privacy Laws

Banks and other financial institutions believe very strongly in protecting consumers' sensitive personal and financial information and their privacy. For hundreds of years, customers have relied on banks to protect the privacy of their financial information. Because banks are literally at the center of people's financial lives, our industry has long been subject to Federal and state data protection and privacy laws. For example, the Gramm-Leach-Bliley Act (GLBA) not only requires financial institutions to protect the security and confidentiality of customer records and information, but it also requires financial institutions to provide consumers with notice of their privacy practices and limits the disclosure of financial information with nonaffiliated third parties.

Banks also are subject to other Federal privacy and data protection laws, including the Right to Financial Privacy Act, the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA). Any Federal data protection and privacy law enacted by Congress must take into account the GLBA and other existing Federal privacy laws and preempt the patch-work of state laws that provide different and often inconsistent consumer protections across the country. Otherwise, a consumer's privacy protections, including their ability to understand their own rights, will depend entirely on the state in which the individual lives.

In enacting the GLBA, it was Congress' intent that a financial institution's privacy practices must be readily accessible and easy to understand ("transparent") so that consumers can make well-informed choices. For example, the GLBA requires financial institutions to provide notice to their customers about their privacy policies and practices. The notice is required to be clear and conspicuous and accurately describe the consumer's right to opt-out of the sharing of personal information with non-affiliated third parties. As a general practice, banks often make these notices easily accessible via websites. Many financial institutions provide these disclosures using a standardized model template designed to follow the same format used for nutrition labeling on food products. Similar transparency should be available to consumers no matter the type of company with whom they do business. For purposes of Federal privacy legislation, the GLBA should be considered a good model for transparency

The GLBA also contains carefully crafted exceptions to the limitations on disclosures to nonaffiliated third parties that are designed to ensure that financial markets that depend on the flow of financial information function efficiently for the benefit of the consumer, the financial institution and the financial markets generally. As a result, it is critical that any new Federal privacy law take into consideration existing privacy laws that apply to financial institutions and avoid provisions that duplicate or are inconsistent with those laws. Any new Federal privacy legislation should recognize the GLBA and other existing Federal privacy laws and preempt the existing patch work of state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system.

B. International and State Privacy Laws

The financial services sector supports an open global economy that enables trade, investment, and growth through the secure and efficient transfer of data across borders. However, measures that dictate where data is stored and how data is transferred can hinder the development of technology infrastructure and reduces our ability to serve our mobile customer base. Measures that "ring-fence" data or require data to remain in the country of origin, often referred to as data localization, ultimately damage the global competitiveness of the U.S. financial services sector and serve as non-tariff barriers to trade. These restrictions limit the efficiency of technology operations, as well as the effectiveness of security and compliance programs. It is unfortunate that the European Union (EU) has chosen to go down this path through its General Data Protection Regulation (GDPR), which has extra-territorial reach that potentially impacts the operations of U.S. banks both internationally and in certain cases, domestically.

The broad and judicially untested language of GDPR may even have an impact on community banks in the U.S. For example, some community banks are starting to question how they can continue to serve academia, military, and non-English speaking communities without running afoul of the GDPR in light of its claim to jurisdiction over people living in the EU and websites offered in an EU language.

For example, existing U.S. customers living, working, or studying abroad, including U.S. college students enrolled at an EU university, academics, or U.S. service members and their families stationed overseas may subject a U.S. bank to GDPR restrictions. Moreover, a community bank in the Southwest offering online banking services in Spanish to a U.S.-based Mexican immigrant community, or a bank in the Northeast offering online banking services to dual U.S.-Portugal citizens that may live, work, retire or own property in both countries may be subject to the GDPR. As a result, the GDPR could potentially reduce the availability of banking services to underserved customers in the U.S.

On the other hand, increasing the global interoperability of privacy regimes can help to mitigate localization requirements while achieving regulatory policy goals. Regional agreements such as the Asia-Pacific Economic Cooperation (APEC) cross-border privacy rule (CBPR) enable commerce supported by the free flow of data, while preserving the national authority to develop privacy requirements that best serve their policy objectives. To date, the CBPR has had diminished utility since it is not global. The financial services sector could potentially support an expansion of CBPR if it includes European Union member states and other key trading partners to effectuate its potential. Similarly, consideration should be given to other well-established privacy principles currently being used by many in the financial sector to ensure interoperability, such as Privacy by Design (PbD), accountability, data retention and use limitations and protection of cross-border transfers of data.

The financial services sector is also concerned that if Congress does not enact uniform national privacy standards, the states will fill the void with a resulting patchwork of disparate and inconsistent requirements. In 2018, California enacted a significant new privacy law, the California Consumer Privacy Act (CCPA). The CCPA was enacted very quickly and without adequate discussion or time to fully understand the consequences.

To its credit, the California legislature included a GLBA exception in recognition of the fact that banks and other financial institutions are already subject to Federal privacy laws. However, concerns remain. For example, the reach of the new law is very broad and will be subject to interpretation in implementing regulations; therefore, its full impact is uncertain. In addition, other states are already considering adopting privacy laws similar to, if not modeled on, the CCPA, and this will exacerbate the existing patch-work of different and often inconsistent state privacy and data breach laws. While these laws may be well-intentioned, they hamper the free flow of data needed to provide consumers and businesses with financial products and services and process financial transactions.

Conclusion

The ABA shares the Committee's goal of protecting sensitive consumer personal and financial information and privacy. Banks and other financial institutions are already subject to the GLBA and other Federal privacy laws. Therefore, any new Federal privacy legislation should recognize the GLBA and other existing Federal privacy laws and preempt the existing patch work of state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO DR. ANDREA JELINEK

Question 1. As I mentioned in the Committee hearing on September 26 regarding the privacy of consumer data, I support privacy rules that afford consumers the same protections no matter where they are in the Internet ecosystem. GDPR and CCPA both appear to take similar approaches. Rather than regulating based on the type of business handling the data, would you agree that regulating and enforcing privacy rules based on the sensitivity of the data collected, used, transferred, or stored is the preferred approach and in the best interest of consumers in terms of certainty and transparency?

Answer. I think that we are living in a society where the processing of personal data is interesting for many businesses, independently of the sector. I believe it is important to offer individuals rights and protection that would apply to all sectors. Having an overarching law does not mean it cannot be complemented by sectorial laws, which take into account the specificities of each field. However, it is important to ensure that such laws specify the rules applicable to each sector, and do not prevent any access of the relevant actors to their agreed basic rights.

In the EU, we have created rules rather based on the notion of risk. One of the considered elements is the nature of the data. Processing sensitive data can give

way to price discrimination practices, based on the profiling of consumers' purchase capacity. It can also lead to manipulation, affecting one's capacity to think freely and, as a result, one's free speech and freedom of opinion. At the end of the day, it can affect human dignity, even when it comes to processing of non-sensitive data.

Question 2. Your testimony highlights the GDPR as a "single set of rules" and a "harmonization of the legal landscape," which "creates a level playing field. . .while guaranteeing the consistent protection of individuals." You state that the uniformity of this approach was intended to reduce compliance costs and increase legal certainty for impacted companies, but more importantly, the consumers these rules are intended to protect. Would you please further describe the utility of this approach compared to a "patchwork" of country-by-country privacy protections?

Answer. I can easily explain the advantages and disadvantages as we have experienced both scenarios. First we had a "patchwork of national laws" (with the Directive) but now we have a uniform approach with the Regulation. Let me first describe the difference between a directive and a regulation. The Directive creates an obligation to respect the rules contained in the national legislation implementing it, but the means used to achieve implementation are not fully harmonised and the different Member States have more flexibility on this regard. This gives Member States the possibility to decide on certain aspects of the directive, as long as the directive's objectives are met, thus potentially leading to a patchworked approach. A Regulation, on the other hand, is directly applicable and requires no transposition. As such, the text of the Regulation applies as it stands (with some, limited exceptions in the case of the GDPR, mainly for areas remaining under the legal competence of Member States).

If you have many national/regional laws with different provisions, the result is a more costly business/legal environment for companies, which have to adapt to different legal frameworks. Even if national/regional laws in different Member States were based on the same directive, it would still lead to differences in terms of compliance, and sometimes companies would likely face duties that would be either incompatible, or very difficult to reconcile. Individuals (including consumers), on the other hand, would be confronted with less certainty, as they are most likely unaware of the provisions that apply in a different Member State. The level of protection could also vary from one legal framework to another. With a regulation, data subjects and consumers know better what they can count on, and so do companies, which have only to apply one law. This is connected to the "one continent, one law" idea, according to which a harmonised legal framework leads to a uniform application and enforcement of rules to the benefit of the EU digital single market. This means one single set of rules for citizens and businesses.

I invite you to consult the European Commission's communication on the GDPR, which offers an overview of the benefits associated with having a Regulation (see here: *https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf*).

Question 3. Mr. Mactaggarts' testimony described the differences between the CCPA and GDPR, and one of the specific points he made was that GDPR's requirement of obtaining consumer's approval before collecting and processing their data would specifically harm "new entrants to the marketplace" since consumers are far less likely to provide up-front consent to newer, lesser-known companies. Do you think Mr. Mactaggart's criticism of GDPR is valid?

Answer. To begin with, consent is only one of the applicable legal basis provided for in the GDPR for the processing of personal data. There are various other options. Therefore, one is not always required to ask for a consumer's approval before collecting and further processing their personal data. On the other hand, data controllers (such as companies) are required to inform data subjects, whose personal data they are processing, in due time. The transparency requirement is important. Said information must include *inter alia* their rights, some of which may include the possibility to object to the processing or even requests for erasure. This is in line with the objectives of the GDPR, foreseen in its Article 1, which concern not only the laying down of rules relating to the free movement of personal data, but also the protection of the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data (Article 8 of the EU Charter of Fundamental Rights).

It is important to add that consent is also not needed, if a company is processing data on behalf of another which received consent for the processing (we refer to them as "processors", whereas in the Privacy Shield, the term used was "agent"). In this situation, a contract has to be signed between the controller and the processor to ensure the necessary level of protection, the security and confidentiality of the processed data and, finally, to ensure that data will not be used for a different

purpose than the one established by the controller. If a consumer is ready to request the services of a new company, the most difficult aspect for a new entrant to the marketplace is to convince an individual to become familiar with, and acquire their product or service, not the request for their consent for processing their personal data.

Question 4. In general, it is obvious that larger companies have sizeable legal departments that enable them to comply with the strict regulations posed by the GDPR and CCPA, but smaller and newer companies likely will not have such resources. Do you have any concerns regarding the significant impact that the enforcement actions related to GDPR compliance could have on small, entrepreneurial businesses?

Answer. The GDPR does foresee such cases, by introducing some flexibility for SMEs. The size of the company will also be taken into consideration by regulators when enforcing certain rules, such as the obligation to keep records (for companies with fewer than 250 employees) or to appoint a data protection officer. Furthermore, the fines, which may be imposed by the supervisory authority in the event of an infringement, are also based on the undertaking's annual turnover and have to be proportionate too.

Question 5. The GDPR included a "data portability" requirement that allows consumers to request and receive their personal information from companies in a structured, commonly used and machine-readable format that can be imported by competing companies and services. Could you please explain what compliance and enforcement with this GDPR provision looks like? Please describe the consumer benefit of this requirement.

Answer. The idea is to enable individuals to receive their personal data, which he or she has provided to the controller and to be able to change providers, in the same way as portability of phone numbers enabled more competition, which worked to the interest of individuals. It is important to add that the direct transmission from one provider to another only applies where it is technically feasible. Moreover, this right supports the free flow of personal data in the EU, avoiding the 'lock—in' of personal data, and encouraging competition between companies. The benefit to data subjects is to make it easier for individuals to switch between different providers, which encourages the development of new services. Enforcement will be ensured by supervisory authorities, as is the case for all data subject rights, although it is for the data controller, in accordance with the principle of accountability, to ensure compliance with this right.

Question 6. Would you expect issues of interoperability to arise for companies aiming to comply with this requirement, especially for smaller businesses that have less resources to change their data practices and equipment?

Answer. The direct transmission and therefore the need for interoperability is not mandatory. It should apply only where it is technically feasible. The GDPR specifies that the data controller has to give back the personal data in a structured, commonly used and machine-readable format. This is normal as, otherwise, the individual would not even be in a position to read the information received that related to him.

Question 7. As GDPR includes requirements like the "right to portability" and the "right to be forgotten," it is clear that these provisions aim to promote the consumer's ownership of their data by requiring companies to abide by their requests to permanently delete or transport their personal data to another company. However, how are these concepts enforced when the consumer's data is submitted as an input to one or multiple proprietary algorithms employed by the company?

Answer. I would like to start by underlining the fact that the right to data portability does not force the company that has paid for the data to delete it from their systems. The right of erasure (also known as the "right to be forgotten") exists, but as a separate right, which the GDPR has balanced against the potential need of a company not to delete the data. When a given processing is unlawful, or the interests of individuals override the interests of the company, personal data should be erased. This is not the case, however, where data should be kept to safeguard free speech, the need to respect history, the processing based on a legal duty, the defense against possible legal claims or the need to keep data for scientific purposes. An example of this is the position of the Advocate General of the Court of Justice of the European Union in the CNIL/Google case (C–507/17).[1] Moreover, the GDPR also

[1] The Advocate General's Opinion is available here (in French): *http://curia.europa.eu/juris/celex.jsf?celex=62017CC0507&lang1=en&type=TXT&ancre=*. A summary, in English, can be found here: *https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002en.pdf*.

takes into consideration the need to respect companies' intellectual property rights. However, this should not be used in a way to develop opaque algorithms that enable decisions to be taken, in an automated manner, against individuals, especially where such decisions can deprive them from specific rights.

In this case, transparency is required to understand the logic of the system, the reasoning of the decision, and also to ask for human intervention. In accordance with the principle of accountability, it is the duty of the controller to implement the necessary safeguards to ensure compliance with the Regulation. This means that, in such cases, the controller needs to ensure that, should such request arise, it can be timely addressed. The specificity of the safeguards to be implemented need to be addressed on a case-by-case basis.

Question 8. Are the outputs of the company's algorithm decidedly the consumer's personal information and required to be deleted or transported at the request of the consumer? If so, do these requirements remain the same if the data outputs are anonymized?

Answer. The right to data portability only applies to personal data. In order to determine whether the output of a company's algorithm is "decidedly" a consumer's personal data (or information), it is necessary to make an assessment in light of the definition of personal data (see Article 4(1) GDPR). Personal data means any information relating to an identified or identifiable natural person. The information does not have to be necessarily linked with the identifiers commonly used in civil society (*e.g.,* name, social security number), but can also be linked to online identifiers (*e.g.,* IP address).

However, it is important to ensure that data is truly anonymized (meaning that you can no longer identify or single out a data subject). Pseudonymised data is still subject to the requirements of the Regulation (see Article 4(5) GDPR for a definition of pseudonymization). The GDPR does not apply to anonymous data.

Please bear in mind that the definition of processing of personal data under the GDPR is quite broad, and, as such, the fact that data are collected as input will fall under said definition in the GDPR.

Question 9. Since companies often use aggregated data outputs to study and improve their existing algorithms, services, and products, what impacts do you expect these GDPR requirements to have on companies' abilities to innovate?

Answer. The GDPR is intended to contribute to the accomplishment of an area of freedom, security and justice, and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons. As such, compliance with its provisions should not have any negative impact on companies' ability to innovate. Trust is of the outmost importance when it comes to innovation. That is what the GDPR aims at providing.

Data protection rules do not aim to prohibit economic activities based on the processing activities, but set out some basic rules of fairness. Up to now, the impact of the GDPR on EU companies has been positive, enabling them to be more in control of their activities and to be in a better position to negotiate with their counterparts. It has also been used to improve consumers' trust.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO DR. ANDREA JELINEK

Question 1. In the EU's GDPR, parental consent is necessary for collection and processing of children's personal data. The law specifically requires "The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology." How do you determine that a reasonable effort has been made?

Answer. Regarding the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action. Therefore, the EDPB recommends the adoption of a proportionate approach, in line with Article 8(2) GDPR and Article 5(1)(c) GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, such as contact details of a parent or guardian.

What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via e-mail may be sufficient. Conversely, in

high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR. Trusted third party verification services may offer solutions, which minimise the amount of personal data the controller has to process itself.

Question 2. In both the EU's GDPR and California's Consumer Privacy Act, parental consent in necessary for collection and processing of children's personal data. Is parental consent an effective model for protecting children?

Answer. This alone is not enough. There is a need to have awareness as well. The child is an individual as anyone else in the GDPR. S/he has a reinforced right to erasure in article 17.1(f) GDPR.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MAGGIE HASSAN TO DR. ANDREA JELINEK

Question 1. GDPR contains provisions outlining the penalties for companies that fail to comply with the regulation. We know that a solid penalty structure should be big enough to be a deterrent and actually adjust companies' incentives appropriately, but not so big that it would be crippling to a small business, whose compliance costs might be a higher percentage of their operating costs than for a bigger company. How and why did the penalties in GDPR come to be structured in their current form?

Answer. Like all corrective measures in general, administrative fines should adequately respond to the nature, gravity and consequences of the infringement, and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, which is either to reestablish compliance with the rules, or to punish unlawful behavior (or both).

Supervisory authorities should identify a corrective measure that is "effective, proportionate and dissuasive".

The GDPR does not make a distinction based on the size of a company, but rather takes into account the risk presented by a given processing operation for the rights and freedoms of the individuals.

Question 2. GDPR, as we all know, strengthens consent requirements. But GDPR also has the potential to address consent fatigue by allowing companies to seek consent only when appropriate, helping ensure that consumers' consent is more meaningful. For example, my understanding is that companies do not need to seek consent for certain uses of data when consent is already implied, such as if the data must be used to fulfill a contract. That makes sense to me, because if consent is sought for everything, it becomes routine and meaningless, whereas seeking consent less frequently makes it more meaningful. Could you comment on this issue of consent fatigue, and how you anticipate addressing this issue under the GDPR?

Answer. The GDPR has made clear that consent can never be implied. Data can be processed according to different legal basis and consent is only one of them. There is a clear distinction between using consent as a legal basis and using a contract as a legal basis.

In the digital context, in light of the volume of information that is required to be provided to the data subject, a layered approach may be followed by data controllers, where they opt to use a combination of methods to ensure transparency. The EDPB recommends in particular that layered privacy statements/notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue.

Layered privacy statements/notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/notice that they wish to read. It should be noted that layered privacy statements/notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/how they can find that detailed information within the layers of the privacy statement/notice. It is also important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO DR. ANDREA JELINEK

Question 1. GDPR Enforcement: The major question that has arisen during these privacy debates is Federal preemption. I certainly understand the desire to avoid a patchwork of state laws but at the same time, we need to ensure that if this is done, enforcement is not delegated to one Federal entity that cannot police the entire digital economy. I understand that GDPR is enforced by 28 different enforcers in the 28 member countries.

Can you talk about how this works and the benefits over a single enforcement entity?

What are the processes by which violations are enforced, do authorities there feel they have the ability to act quickly and effectively against violators?

Answer. All supervisory authorities have enforcement powers on their own territory. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the European Union. For that purpose, the supervisory authorities shall cooperate with each other and the European Commission.

When there is a cross border processing, a "lead supervisory authority" is the authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data.

The lead supervisory authority will coordinate any investigation, involving other "concerned" supervisory authorities.

Identifying the lead supervisory authority depends on determining the location of the controller's "main establishment" or "single establishment" in the EU.

The essence of the lead authority principle in the GDPR is that the supervision of cross-border processing should be led by only one supervisory authority in the EU.

The EDPB acknowledges that fining powers represent for some national supervisory authorities a novelty in the field of data protection, raising numerous issues in terms of resources, organization and procedure. The GDPR requests Member States to ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

Question 2. Physical Security of Data Centers: One of the things we often don't think about when we talk about privacy is that when data is stored, it is actually present somewhere at a physical location. Apple has a data center located just east of Reno and in Las Vegas, and we have an expansive company called Switch which designs, constructs and operates data centers. As we think about privacy and data security, it is important to keep in mind how we're securing these locations from physical and cyber-attacks. Question 1. Does GDPR, or any other European law, address this issue?

Answer. Yes, it has consecrated the integrity and confidentiality of the data as a core principle of data protection. As such, personal data need to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR requests the controller and processor to take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The controller and the processor shall also implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Article 32 GDPR provides for examples of such technical and organisational safeguards.

Question 3. Selling Versus Leveraging Data: Facebook, Google, and other companies with similar business models do not sell data, but rather they leverage data to sell advertisements. An advertiser approaches an edge provider with an audience it would like to reach and the edge provider uses the data it maintains to match the ad to the desired audience. The fact that the data do not change hands is immaterial for consumers' experience, but it still is a distinction that various laws treat differently. I think when we talk about giving consumers notice about how data is used, intricacies like this can be difficult to explain in the context of a notice and consent model. How do lawmakers in Europe think about this distinction?

Answer. The GDPR applies to activities that involve the processing of personal data. In these cases, as long as personal data has been processed, the GDPR applies. However, its application needs to be framed in accordance with the purpose of the

processing, the legal basis, the role played by the different actors in the different processing operations as well as by their territorial location.

The GDPR contains strict provisions on the relationship between joint controllers and controllers/processors, as well as on transfers of data outside of the EU.

In addition, the GDPR provides for a purpose limitation principle, according to which data cannot be further processed in a manner that is incompatible with the original purpose for which it was collected.

In the context of a notice and consent model (as understood from a GDPR perspective), the reuse by a given controller/processor of the data originally collected can only occur in two cases: either the consent has been originally and explicitly requested, or a new consent is required. The conditions for having a valid consent have been reinforced under the GDPR and the individual has always the right to withdraw his/her consent at any time.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO ALASTAIR MACTAGGART

Question 1. As I mentioned in the Committee hearing on September 26 regarding the privacy of consumer data, I support privacy rules that afford consumers the same protections no matter where they are in the Internet ecosystem. GDPR and CCPA both appear to take similar approaches. Rather than regulating based on the type of business handling the data, would you agree that regulating and enforcing privacy rules based on the sensitivity of the data collected, used, transferred, or stored is the preferred approach and in the best interest of consumers in terms of certainty and transparency?

Answer. We take a slightly different approach, for the following reason: what's sensitive to you, may not be to me, and vice versa. Say Aunt Sadie rarely leaves her retirement community—she might not consider her geolocation sensitive. A sitting U.S. Senator would probably feel the opposite way. Laura might not care if her browsing history is disclosed; Alice might be trying to get pregnant, and would hate a prospective employer learning that fact.

We think it's more practical to treat all personal information as, well, personal. It's your information. CCPA allows you to find out what has been collected ('Right to Know'); to decide whether it can be sold ('Right to Say No'); and to know it will be kept safe ('Right to Data Security').

The approach we have taken is, indeed, similar to GDPR, but whereas their approach is based on 'Notice and Consent,' CCPA's architecture relies on giving individuals the power to 'Opt-Out.' (Incidentally, we feel giving consumers choice, as opposed to requiring all businesses to always get consent, is more in keeping with a typical American ethos of individual responsibility).

We don't regulate "types" of business, we regulate only large businesses and data brokers doing business in the state of California. We give people the right to control what is done with their information, and we think simplicity is one of the best features of our law (easier for the consumer to understand, and easier for the business to comply with).

Question 2. The CCPA defines "personal information" to mean "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked directly or indirectly with a consumer or household." Are you concerned that the CCPA's extremely broad definition of "personal information" sweeps in information that isn't even sensitive? Additionally, what does it mean that information can be "linked . . . indirectly with a consumer or household?"

Answer. California Civil Code 1798.80(e), existing California law for almost two decades [1] prior to the passage of CCPA, defines "personal information" as:

> (e) "Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual . . ."

We chose our definition to track this code section, and included the phrase "or could reasonably be linked directly or indirectly with a consumer or household," for the reasons set forth below. (Note that we think the word 'reasonably' appropriately limits the scope of this additional phrase.)

As set out in the answer to the first question, CCPA does not distinguish between 'sensitive' and 'other' personal information, because what is not sensitive to one consumer, might be to another. CCPA's approach is that consumers' personal information is all equally covered by the law.

---

[1] *California Assembly Bill 2246, 9/30/2000*

Recall, however, that if companies are not using personal information to track individual consumers—if, for example, they de-identify the information—then under the definitions in CCPA, such information is no longer considered personal information, and therefore not covered by CCPA.

The best rationale for including "information that can be linked indirectly to a consumer or household," is set out in the famous 2012 New York Times Target[2] story. In this classic and early example of the power of the algorithm, Target tracked women's purchase histories, and cross-referenced them with women who had started a baby shower gift registry. By analyzing thousands of data points, Target was able to determine which women were pregnant merely by their purchase of items like certain lotions, soaps, and cotton balls. Not only that, but Target was able to predict their due date accurately, all without any input from the woman being tracked and analyzed.

In the article, Target started sending pregnancy coupons to a teen, angering her father, who was in the dark about the pregnancy.

No one had told Target the girl was pregnant—the algorithm had determined, indirectly, that she was pregnant.

One can imagine scores of such examples, given the continued explosion in computing power, and the vastly increased efficiency of algorithms. If Frank is in the market to buy life insurance, does he want the life insurer to charge him extra based on their analysis of how many times his car or phone stops at a fast food restaurant? If Nancy wants to get a mortgage, is it fair that she pays more if the lenders think she's at risk of losing her job if she gets to work at 10 each day (even though she might have an understanding with her boss that she can work from home in the morning to skip traffic)?

For this reason, we included the 'linked directly or indirectly' concept, since it's clear that technology has advanced dramatically in the 19 years since the definition in Cal Civil Code 1798.80 was passed into law.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TOM UDALL TO ALASTAIR MACTAGGART

Question. In both the EU's GDPR and California's Consumer Privacy Act, parental consent in necessary for collection and processing of children's personal data. Is parental consent an effective model for protecting children?

Answer. Verifiable parental consent is already a necessary and important step when collecting 'personal information' from children under 13 in the U.S. under COPPA. The CCPA expands this right to Californians under the age of 16. While parental consent is an important consideration, it doesn't solve the issue that, even for adults, websites terms and practice are difficult to understand and even more difficult to say no to.

We forecast that social pressure will compel the adoption of laws that require businesses aimed at children to limit their data collection to the minimum personal information necessary to offer the business, game or app. This is a well-known principle called 'privacy by design,' and we think it should be the default for all younger consumers, especially those under 18.

We believe that both parental consent and data minimization/privacy by design are important factors in any comprehensive privacy regime. When drafting CCPA, we took the approach that some progress is better than none, and we are thrilled that we were able to better protect more children.

Nothing could be more important. With a recent study showing almost 6,000 of the most popular children's Android[1] apps were potentially in violation of the Child Online Privacy Protection Act (COPPA), it is clear business needs additional regulation to safeguard children.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MAGGIE HASSAN TO ALASTAIR MACTAGGART

Question 1. CCPA contains provisions outlining the penalties for companies that fail to comply with the law. We know that a solid penalty structure should be big enough to be a deterrent and actually adjust companies' incentives appropriately, but not so big that it would be crippling to a small business, whose compliance costs might be a higher percentage of their operating costs than for a bigger company.

---

[2] How Companies Learn Your Secrets, New York Times Magazine, Feb 16, 2012

[1] (Reyes, April 25, 2018) Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. Berkeley Laboratory for Usable and Experimental Security.

How and why did the penalties in CCPA come to be structured in their current form?

Answer. CCPA contains different penalties for different violations.

(1) With respect to data breaches, it is important to remember that covered businesses can rely on *multiple* steps to reduce or eliminate financial liability for data breach, including (1) encrypting a consumer's data; (2) redacting a consumer's identifying information from the data; or (3) taking steps to comply with existing California data protection law (which well predated CCPA). With respect to this third step, the California Code section has long required that [California Civil Code 1798.81.5 (b)] "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Instituting these reasonable procedures and practices could eliminate a business's financial liability under the data breach section.

[Note: we assume the California Attorney General, the rulemaking authority under CCPA, will issue regulations defining the precise standards to apply to encryption, redaction, and "reasonable security procedures and practices." If a business wants to rely on these steps to reduce or eliminate its financial liability in the event of a data breach, the steps must represent effective and meaningful consumer protections, and not simply be avenues for unscrupulous businesses to avoid the reach of the law.]

If, on the other hand, a business had ignored all of these 'protections' against financial liability in the event of a data breach, then it would face financial liability of from $100 to $750 per consumer per incident, or actual damages, whichever was greater. This amount was selected because it could amount to a total that would impose a realistic check on businesses that simply ignore consumer data protection.

Another important aspect of the penalties involving data breach is that they only apply to a subset of personal information, *i.e.,* not all personal information as defined in CCPA. The information covered in the data breach provision is defined in 1798.81.5(d)(1)(A),[2] and is essentially a more sensitive subset of personal information. Part of the approach here was that it felt more appropriate to have serious financial consequences subject to a private right of action, for situations involving the theft of sensitive personal financial and health information, than it did in a situation where for example a company had perhaps inadvertently failed to disclose to a consumer all the personal data it had about that consumer pursuant to the Right to Know.

Finally, please note that CCPA specifically includes language in 1798.150(a)(2) allowing a court to reduce the award based on the "nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth." It was important to the drafters that this financial penalty provision be flexible enough to address the nature of the breach, after judicial review.

(2) With respect to all other violations, the Attorney General has the ability to enforce and impose penalties of not more than $2,500 per violation, and up

---

[2] 1798.81.5(d)(1)(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social security number.

(ii) Driver's license number or California identification card number.

(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information.

(B) A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

(2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

(3) "Health insurance information" means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

to $7,500 per intentional violation. These fines are drawn from existing penalties for violations of California's Unfair Competition Law, which authorizes fines of $2,500 per violation and up to $6,000 for violations of injunctions. Additionally, the business has a 30-day right to cure the violation after being notified by the AG, which again seemed like the sensible, moderate approach to take.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO ALASTAIR MACTAGGART

Question 1. Selling Versus Leveraging Data: Facebook, Google, and other companies with similar business models do not sell data, but rather they leverage data to sell advertisements. An advertiser approaches an edge provider with an audience it would like to reach and the edge provider uses the data it maintains to match the ad to the desired audience. The fact that the data do not change hands is immaterial for consumers' experience, but it still is a distinction that various laws treat differently. I think when we talk about giving consumers notice about how data is used, intricacies like this can be difficult to explain in the context of a notice and consent model. How do lawmakers in California think about this distinction?

Answer. This entire area contains a couple of intricate distinctions, as you point out, but they are important so let me address them separately.

(1) Third party tracking. While Facebook and Google do not "sell" data in the traditional sense, they certainly "buy" it in terms of acquiring it by tracking most people across most websites in the world and by paying outside data brokers to provide information about their users.[3] Their ability to create deep, longitudinal profiles on consumers depends very materially on their ability to track you wherever you go, even if you are not logged into their services, or have never created an account with them. CCPA's framework gives consumers the ability to stop their browsing history being vacuumed up and used by these large data miners across their platforms.

(2) While these companies may not 'sell' data in a manner that a traditional data broker does, their ability to offer advertisers increasingly 'thin' consumer slices, renders this distinction moot. Thus, if an advertiser wants to reach single, gay, Latino attorneys with one child under 5, living in California, on Facebook; and if a consumer clicks on the ad targeted at this group, then the advertiser has a virtually perfect idea of the demographic makeup of the consumer. Across a moderately large group, the errors are minimized, and so while Facebook does erect an initial hurdle to a direct 'sale' of the consumer's data, at some point the distinction between selling and not selling, is semantic. Some in the privacy community call this phenomenon, "leakage."

(3) CCPA accepted this concept of "leakage" as a necessary by-product of permitting advertising (which our law does). Importantly, however, CCPA constrains the further use by the advertiser of the personal information, if the consumer has opted-out of the sale of their information: it cannot be resold, or reused outside of the context in which it was collected.

(4) We think CCPA arrived at a good middle-ground in this difficult-to-regulate-well area: the law dramatically restricts the unconstrained sale of consumers' personal information, for consumers who have opted out of the sale of their information. Yet it permits advertising, which we felt was important as it remains for the most part the economic engine of the internet, and of many free services offered to consumers.

Question 2. Privacy Enhancing Technology: The major theme of this debate has been how technology has changed the relationship between the consumer and their expectation of privacy. In general, we have talked about how technology can enable more and better information for consumers while at the same time jeopardizing their privacy. But at the same time, technology can also enhance privacy. Encryption, anti-virus, cybersecurity technologies are all examples of this. Did this come up in any of the discussions surround the California law?

Answer. Absolutely, this question is spot-on with respect to the meme that the technology industry would like to propagate. Their pitch is that without the ability to track you at all times, across all your devices, they won't be able to offer you 'the

---

[3] *https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them*

services you like and love.' Or, even better, that they won't be able to offer you the 'relevant ads' that you want to see.

In all our research, we have never encountered one consumer who said they had a problem with ads not being accurate enough. On the contrary, for many consumers the 'ick factor,' or creepiness level, is at its highest when they browse for a product on one device, on one platform, and then minutes later on a different device and platform, 'the algorithm' has found them and starts advertising to them. You're looking at an article on Machu Pichu on your desktop browser; ten minutes later in the elevator, your Facebook page shows an ad for travel to Machu Pichu.

Since CCPA's passage, I have been contacted by numerous companies who say that their company and technology can solve any of CCPA's current requirements. I think the innovation in business models and privacy preserving technologies this law will help foster will dwarf any loss of convenience or ease-of-use for consumers using technology (to be blunt, I think there will be no such loss).

Auto-safety requirements fostered a revolution in auto technology (air bags, ABS braking, heads-up-display, tire pressure monitoring, etc.). Energy efficiency standards in building have revolutionized that business—think of low-E glass, better insulation, solar panel costs dropping while efficiency rose. Privacy is no different, and CCPA will help spur a huge transformation in managing consumers' personal information.

Question 3. How do you think we can help develop these technologies at the Federal level?

Answer. We at Californians for Consumer Privacy have tremendous faith in American innovation, and the free-enterprise model. We think by far the best approach is for government to determine outcomes—what basic consumer privacy expectations can and should be—and then let private markets develop a solution to best achieve that outcome.

We think government works best when it regulates—something it is inherently suited for—but that it gets more difficult if the regulator attempts to pick winners and losers.

That said, we also think it is *highly important* that whoever the regulator is (we assume the FTC), it be given rulemaking authority, as well as the power to enforce and issue fines, *without* relying on a 2-strikes-and-you're-out model.

Question 4. Federal Preemption: Technology companies make the argument that one single, national standard would make the most sense in the United States because a patchwork of 50 different laws would not work to regulate something as fluid as data.

Are there any circumstances under which you would be in support of Federal preemption of state privacy laws?

Answer. As a general matter, CCPA's position is that any Federal legislation should be a floor, not a ceiling, just as it is for example with Gramm-Leach-Blilely, another Federal privacy law. If states want to continue to innovate, we see that as a positive for consumers.

Also, we want to push back on the 'unworkability' narrative being propounded by the large technology platforms.

Imagine the complexity of building a large high-rise: getting calculations wrong could cause potentially thousands of deaths. Yet the states by and large have different building codes.

Physicians—also an occupation where mistakes can be lethal—are licensed by the states.

And around the country, buildings are being built successfully, and sick patients are being cared for and cured.

The point is, CCPA's basic premise is that large businesses comply with thousands of different local policy regimes, opening/closing hour restrictions, zoning and planning laws. This ecosystem, while complex, also promotes policy innovation and allows the states to experiment with different approaches to find the most ideal solution for all stakeholders. While we have no wish to promote complexity, we think a robust Federal privacy law that was the floor, not the ceiling in terms of consumer privacy protection, is totally workable. Many states will not choose to go further, if the Federal law is strong enough. Some states will, and businesses will make a one-time adjustment to doing business under new laws, and move on.

However in the final analysis: if there were a fabulous, effective, robust Federal privacy law, which had adequate enforcement (we suggest at a minimum allowing all State Attorneys General, plus all City and County District Attorneys for cities or counties with over 500,000 residents, to enforce any Federal privacy law), where the regulator had ample, independently-guaranteed funding, and effective rule-making authority, so that the law could change with the times, and there were provi-

sions put in place so that enforcement was non-political, we think that could be a good thing for the country.

Question 5. Data Protection Officers: As you well know under Europe's GDPR there is a requirement that any entity that handles large amounts of data appoint a Data Protection Officer, or DPO. DPO's are responsible for educating the company on compliance, training staff in data processing, providing advice on data protection, and so on. What is your perspective on this requirement?

Answer. In some respects, this person would be the equivalent of the Chief Privacy Officer that most large companies in this country have.

However for such a position to be meaningful, it would require the existence of effective laws underpinning consumer privacy. We think CCPA is the first major step in this direction, in this country, and it (or GDPR in the EU) will give the CPO or DPO, as the case may be, the ability to hold his or her ground within the organization, and hopefully not be regarded as 'just' a cost center.

So working together with effective legislation, we think the DPO position referenced above will be almost a de facto requirement in any covered business under CCPA.

Of note, one item we lost along the way during our negotiations as the initiative moved to a law: the initiative had a whistleblower provision, which would have protected any insider coming forward with non-public information. This is a very real concern—for example, I spoke with the Global Data Privacy Officer at one of the largest and most prominent multinational consulting firms, and her only real criticism of CCPA was that we did not have a whistleblower provision, as she has seen firsthand (not at her firm) how large companies will try to pursue employees committed to doing the right thing, if a company thinks such a course of action will hurt their bottom line.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO LAURA MOY

Question 1. In both the EU's GDPR and California's Consumer Privacy Act, parental consent in necessary for collection and processing of children's personal data. Is parental consent an effective model for protecting children?

Answer. Parental consent is necessary, but not sufficient, to protect children. The parental consent model helps to increase parental awareness of what information online sites and services will collect about their children and for what purpose, which is important for parents to understand. At least in theory, the parental consent model also helps provide opportunities for parents to permit or either permit or prohibit certain uses of their children's information.

In addition to parental consent requirements, policymakers should consider supporting additional privacy rights that help protect children. For example, access and deletion rights—which may be important for all consumers to have—are of particular value to children, whose both cognitive and judgment abilities are not fully developed. In an era of inexpensive and sometimes indefinite storage, policymakers must take steps to ensure that information shared online by consumers—especially children—does not unfairly haunt them for the rest of their lives.

Question 2. A recent *New York Times* analysis found that both the Apple App Store and the Google Play Store have apps in their respective children's or family sections that potentially violate Children's Online Privacy Act (COPPA).[4] What specific role should platform owners play to ensure compliance on their platforms?

Answer. If we allow app platform owners to hide behind ignorance as an excuse for privacy violations, we will only reinforce those platform owners' incentives to look the other way when privacy violations are taking place on their platform. App stores that promote sections of their store as child-directed—as both Apple and Google do—should take steps to ensure that apps in that section are not engaging in data practices that violate children's privacy expectations and laws. In addition to scrutinizing app platforms' behavior in this matter under COPPA, enforcers should also scrutinize these platforms' behavior under prohibitions against unfair and deceptive trade practices. Marketing apps as child-appropriate through an app store without taking steps to stop widespread COPPA violations by those apps may constitute an unfair and/or deceptive trade practice, even independently of COPPA.

---

[4] Valentino-DeVries, J., Singer, N., Krolick, A., Keller, M. H., "How Game Apps That Captivate Kids Have Been Collecting Their Data." The New York Times. 2018, September 12. *https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html*

The widespread existence of child-targeted apps that potentially violate COPPA is also indicative of failures by enforcers—including the Federal Trade Commission—to adequately enforce the law. When app developers list their apps in the children's section of a store, those apps should be presumed to be child-targeted, and held strictly to COPPA standards.

Question 3. It seems hard to achieve compliance if the large tech platforms have no responsibility or liability for apps they are hosting, especially when these apps can be put there by fly-by-night operators overseas who do not care if they are in violation of U.S. law. What rules and enforcement should the U.S. have in place to ensure that the big tech platforms are properly protecting children's privacy?

Answer. Congress should consider vesting the Federal Trade Commission or another expert agency with expanded authority and tools to go after big tech platforms and other companies for engaging in harmful commercial data practices. It is of crucial importance that an expert agency have strengthened authority to prohibit unfair and deceptive trade practices; rulemaking authority over data security, data brokers, and consumer privacy; and strong tools to vigorously enforce the law—including with the ability to fine companies for privacy and data security violations. There is little incentive for companies to abide by children's privacy laws if those laws are not vigorously enforced.

Question 4. Since COPPA was enacted, the FTC has only brought 28 COPPA cases with over 10 million in civil penalties, what changes should be made to the legislation or the regulation to ensure more vigorous enforcement?

Answer. The FTC has not done enough to protect children's privacy. Part of the reason for this is that the agency simply does not have sufficient resources to do its job. The number of online sites and services has increased exponentially over the past twenty years, and the FTC has not been able to keep up. It is not beneficial to consumers for the FTC to be tasked with enforcing COPPA if the agency is not given the staff and resources it needs to do that job well.

If enforcers like the FTC and state attorneys general are not going to be able to vigorously enforce the laws they are expected to enforce, Congress should consider updating those laws to provide a private right of action so that users can initiate enforcement on behalf of themselves.

Question 5. Do you think the COPPA Safe Harbor program is effective in ensuring that children's privacy is protected? Why or Why not?

Answer. Critics of the COPPA safe harbor have said that safe harbor programs do not do enough to ensure that program participants remain in compliance with the law, but that the FTC seldom revokes safe harbor status for programs that fail to police participants. I am not an expert in the COPPA safe harbor, but in general safe harbor programs should 1) only shield participants from enforcement to the extent necessary to create incentives for participation (*i.e.,* enforcers should still be able to take some action against participants who nevertheless violate the law), and 2) entail a rigorous certification process that ensures rubber stamp programs will not receive safe harbor status.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO LAURA MOY

Question 1. Selling Versus Leveraging Data: Facebook, Google, and other companies with similar business models do not sell data, but rather they leverage data to sell advertisements. An advertiser approaches an edge provider with an audience it would like to reach and the edge provider uses the data it maintains to match the ad to the desired audience. The fact that the data do not change hands is immaterial for consumers' experience, but it still is a distinction that various laws treat differently. I think when we talk about giving consumers notice about how data is used, intricacies like this can be difficult to explain in the context of a notice and consent model. How should we think about this distinction?

Answer. Yes, often uses of data are problematic even when the data at issue does not change hands from one party to another. This is one reason that I have advocated for a privacy model that defines affirmative obligations that attach whenever consumer data is collected or used. I am attaching here the comments I recently filed in response to the National Telecommunications and Information Administration's (NTIA) request for public comments on proposed user-centric privacy outcomes and high-level goals that should guide this Administration's approach to consumer privacy in the near future. In my comments, I argue in favor of affirmative obligations based on the Fair Information Practices (FIPs). I also urge the NTIA additionally to recognize that certain uses of consumer data, such as discrimination, simply

should not be allowed. In addition, I encourage NTIA to include purpose specification and use limitation among its list of desired privacy outcomes.

Question 2. Privacy Enhancing Technology: The major theme of this debate has been how technology has changed the relationship between the consumer and their expectation of privacy. In general, we have talked about how technology can enable more and better information for consumers while at the same time jeopardizing their privacy. But at the same time, technology can also enhance privacy. Encryption, anti-virus, cybersecurity technologies are all examples of this. How do you think we can help develop these technologies at the Federal level?

Answer. Encryption, anti-virus, and cybersecurity technologies all enhance data security. To encourage development of these technologies, regulators should ensure that companies have strong incentives to improve data security. Data security standards must be meaningful and enforcement agencies must have sufficient staff, resources, and authority to hold companies to those standards.

Question 3. Federal Preemption: Technology companies make the argument that one single, national standard would make the most sense in the United States because a patchwork of 50 different laws would not work to regulate something as fluid as data. Are there any circumstances under which you would be in support of Federal preemption of state privacy laws?

Answer. The fact that state legislatures are passing privacy laws is indicative of the fact that those states' constituents are demanding stronger privacy protections. Indeed, people across the country are concerned about privacy and asking regulators to step in to do something about it. That may be an argument in favor of creating a strong Federal standard, but it is not an argument in favor of doing away with state laws. Congress should look to states to help understand how state legislatures help protect consumers, not only by instituting strong substantive standards, but also by demonstrating agility and a quick-response ability that simply is not possible at the Federal level. Federal law should be informed by, and should not eliminate, these important benefits to consumers.

Question 4. Data Protection Officers: As you well know under Europe's GDPR there is a requirement that any entity that handles large amounts of data appoint a Data Protection Officer, or DPO. DPO's are responsible for educating the company on compliance, training staff in data processing, providing advice on data protection, and so on. What is your perspective on this requirement?

Answer. There is a lot of wisdom in requiring every entity that collects or uses private consumer data to appoint an individual responsible both for counseling the entity on privacy internally, and for serving as a liaison between regulators and the entity.

Question 5. Notice and Consent: The notice and consent model, while helpful, is not a silver bullet. Consumers are likely to click through and face decision fatigue about the many different privacy policies on every different platform. From your perspective, what data practices, if any, should be prohibited in general?

Answer. I have argued in the past that some uses of data simply should not be allowed. Chief among these are discriminatory uses. The information that Americans share online should not be used to selectively deny them access to—or awareness of—critical opportunities, especially things like housing, education, finance, employment, and healthcare. It should not be used to amplify hate speech. It should not be used to enable data brokers to secretly build ever-more-detailed consumer profiles that they then turn around and sell, unrestricted, to the highest bidder. Privacy should actively protect Americans from the most harmful uses of their information.

I am attaching here the comments I recently filed in response to the National Telecommunications and Information Administration's (NTIA) request for public comments on proposed user-centric privacy outcomes and high-level goals that should guide this Administration's approach to consumer privacy in the near future. These comments provide a little more detail on this point.

BEFORE THE

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

In the Matter of	)	
	)	
Developing the Administration's	)	Docket No. 180821780–8780–01
Approach to Consumer Privacy	)	
	)	

COMMENTS OF CENTER ON PRIVACY & TECHNOLOGY AT GEORGETOWN LAW

TABLE OF CONTENTS

I. Introduction and Summary

The Center on Privacy & Technology at Georgetown Law is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for public comments (RFC) on proposed user-centric privacy outcomes and high-level goals that should guide this Administration's approach to consumer privacy in the near future.[1]

The Center on Privacy & Technology generally supports NTIA's proposed privacy outcomes and proposed high level goals for Federal action on privacy. In addition, however, the Center on Privacy & Technology urges NTIA to move further in the direction of strong consumer protection by recognizing additional important privacy outcomes and high-level goals for Federal action, and by approaching calls for a risk-based approach and harmonization with caution. In particular, NTIA should:

- Assert explicitly and forcefully that transparency and control—or notice and consent—alone are insufficient to protect consumers in the 21st century.
- Include non-discrimination among its list of desired privacy outcomes.
- Include purpose specification and use limitation among its list of privacy outcomes.
- Recognize that privacy violations themselves are harmful, and not support a privacy framework that conditions privacy obligations on the outcome of an assessment of risk of tangible secondary harms to individual users.

[1] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (Sept. 26, 2018) [hereinafter RFC].

- Not support regulatory "harmonization" at the expense of context-specific privacy.
- Not support regulatory "harmonization" at the expense of strong existing protections.
- Identify strong privacy enforcement authority as a goal for Federal action.
- Identify regulatory agility as a goal for Federal action.

II. Notice and Consent, While Necessary, Are Not Sufficient to Protect Consumers in the 21st Century

The Center on Privacy & Technology agrees with NTIA that while transparency and control are important privacy outcomes for any Federal action on privacy, more is needed. Consent today is less meaningful than it once was. It is increasingly difficult for consumers to understand the many ways in which their information might be collected, what that information might reveal about them, and how it might be used.

Even when they are given information about how companies will handle their data, Americans often lack sufficient choice to be able to exercise meaningful control over their data. As dominant providers of online services have grown, expanded partnerships with other services, and become integrated with everyday communications, they have become an unavoidable part of consumers' lives. In addition to rendering consent mechanisms illusory, this amplifies societal vulnerability to harms perpetrated by tech giants. Consumers now find that they effectively have no choice but to use services provided by—and share their data with—a handful of these large companies.

For example:

- The cost disparity between Apple and Android devices drives many low-income consumers to Android-powered devices, subjecting them to greater tracking by Google and less privacy-enhancing encryption defaults.[2]
- On the web, consumers cannot avoid being tracked by Google's pervasive analytics and advertising networks.[3]
- In some instances, employers require employees to have accounts through tech giants such as Facebook.[4]
- Amazon is putting local retailers and booksellers out of business, limiting offline options for consumers to purchase certain goods. The platform is also positioning itself as the platform through which cities, counties, and schools purchase office and classroom supplies, leaving retailers with little choice other than to use Amazon to reach government buyers.[5]
- In order to get online, consumers have no choice but to share vast amounts of information about their online activities and associations with an Internet service provider—of which there may only be one or two possible options in any given location.

And even if consumers later become dissatisfied with the practices of a provider, it can be extremely difficult to switch to another provider. Not only are there limited alternatives available, but once an individual establishes an account with a provider and uses that account to create and store information, it may not be possible for the consumer to take that information elsewhere.

---

[2] *See Christopher Soghoian: Your Smartphone Is a Civil Rights Issue,* Tiny Ted, *https://en.tiny.ted.com/talks/christopher_soghoian_your_smartphone_is_a_civil_rights_issue.*

[3] According to one report, Google Analytics is present on 56 percent of all websites. W3Techs, *Usage Statistics and Market Share of Google Analytics for Websites, https://w3techs.com/technologies/details/ta-googleanalytics/all/all* (last visited Aug. 19, 2018).

[4] Landan Hayes, CareerBuilder, *Not Getting Job Offers? Your Social media Could Be the Reason,* Aug. 9, 2018, *https://www.careerbuilder.com/advice/not-getting-job-offers-your-social-media-could-be-the-reason* ("Nearly half of employers (47 percent) say that if they can't find a job candidate online, they are less likely to call that person in for an interview"); *see* Laura Fosmire, *Senate Moves Forward on Social Media and Employment Bill,* Statesman J., Mar. 4, 2015, *https://www.statesmanjournal.com/story/money/business/2015/03/04/senate-moves-forward-social-media-employment-bill/24359757/;* Kashmir Hill, *Beware, Tech Abandoners. People Without Facebook Accounts Are 'Suspicious,'* Forbes, Aug. 6, 2012, *https://www.forbes.com/sites/kashmirhill/2012/08/06/beware-tech-abandoners-people-without-facebook-accounts-are-suspicious/#2d7072ca8f95.*

[5] Olivia LaVecchia & Stacy Mitchell, *Amazon's Next Frontier: Your City's Purchasing* (2018), *https://ilsr.org/wp-content/uploads/2018/07/ILSR_AmazonsNextFrontier_Final.pdf;* Abha Bhattarai, *How Amazon's contract to sell office supplies to cities could hurt local retail,* Wash. Post, July 10, 2018, *https://www.washingtonpost.com/business/2018/07/10/amazon-now-sells-office-supplies-books-thousands-cities-other-local-organizations/.*

Federal action on privacy—whether principles or legislation—should therefore recognize that a framework premised on notice and consent alone is insufficient to protect consumers. NTIA's proposed approach is consistent with this idea and includes additional privacy outcomes. The Center on Privacy & Technology urges NTIA to go one step further and to acknowledge explicitly and directly that notice and consent are not sufficient to protect consumers.

III. Privacy Outcomes Should Include Affirmative Obligations that Attach Whenever Consumer Data Is Collected or Used

Beyond the need for greater transparency and control, NTIA names reasonable minimization, security, access and correction, risk management, and accountability as important privacy outcomes. The Center on Privacy & Technology generally supports these additional outcomes, and urges the NTIA additionally to recognize that certain uses of consumer data, such as discrimination, simply should not be allowed. The Center on Privacy & Technology also encourages NTIA to include purpose specification and use limitation among its list of privacy outcomes.

A. NTIA Should Clearly Assert that Some Uses of Data Simply Should Not Be Allowed

Any list of privacy outcomes should include a recognition that some uses of data simply should not be allowed. Chief among these are discriminatory uses. The information that Americans share online should not be used to selectively deny them access to—or awareness of—critical opportunities, especially things like housing, education, finance, employment, and healthcare. It should not be used to amplify hate speech. It should not be used to enable data brokers to secretly build ever-more-detailed consumer profiles that they then turn around and sell, unrestricted, to the highest bidder. Privacy should actively protect Americans from the most harmful uses of their information.

NTIA should, specifically, enumerate non-discrimination among any list of desired privacy outcomes released by the agency. There is much work to do in this area; at present, discriminatory uses of information are widespread. For example, Facebook made assurances in 2017 to tackle discriminatory advertising on its platform after facing public outrage and pressure from advocates regarding its "ethnic affinity" advertising clusters, but the Washington State Attorney General found that it was still possible to exclude people from seeing advertisements based on protected class membership.[6] Civil rights organizations are also suing Facebook for enabling landlords and real estate brokers to exclude families with children, women, and other protected classes of people from receiving housing ads.[7]

Discrimination also occurs in the targeting of employment advertisements. Advertisers can use Facebook's algorithm to target job ads to certain genders, often along gender stereotypes.[8] The systematic targeting and exclusion of communities can also be a byproduct of algorithmic content and ad distribution that optimizes for cost-effectiveness and user "engagement," which can lead to distribution that is discriminatory in impact, if not intent.[9] For example, algorithms seeking the best returns on optimized ads displayed more ads for science, technology, engineering and mathematics opportunities to men than women.[10]

Digital data and services should operate as tools to advance opportunities and equity, rather than to reinforce existing social disparities. Federal action on privacy therefore must seek to ensure that users' data is not used to exclude users from

---

[6] Sam Machkovech, Facebook Bows to WA State to Remove "Discriminatory" Ad Filters, Ars Technica, July 25, 2018, *https://arstechnica.com/information-technology/2018/07/facebook-bows-to-wa-state-pressure-to-remove-discriminatory-ad-filters/*.

[7] Nat'l Fair Housing Alliance, *Facebook Sued by Civil Rights Groups for Discrimination in Online Housing Advertisements* (Mar. 27, 2018), *https://nationalfairhousing.org/2018/03/27/facebook-sued-by-civil-rights-groups-for-discrimination-in-online-housing-advertisements/*.

[8] Women were excluded from seeing Uber driver, truck driver, and state police positions but targeted for nurse openings. *See* Ariana Tobin and Jeremy B. Merrill, *Facebook Is Letting Job Advertisers Target Only Men,* ProPublica, Sept. 18, 2018 *https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men.*

[9] *See* Anja Lambrecht & Catherine E. Tucker, *Algorithmic Bias? An empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads* (Mar. 9, 2018), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260* (finding that because younger women are an expensive demographic to show ads to, "An algorithm which simply optimizes cost-effectiveness in ad delivery will deliver ads that were intended to be gender-neutral in an apparently discriminatory way, due to crowding out."): Latanya Sweeney, *Discrimination in Online Ad Delivery,* Communications of the ACM, May 2013, at 44, *https://cacm.acm.org/magazines/2013/5/163753-discrimination-in-online-ad-delivery/*.

[10] Dina Fine Maron, *Science Career Ads Are Disproportionately Seen by Men,* Scientific American, July 25, 2018 *https://www.scientificamerican.com/article/science-career-ads-are-disproportionately-seen-by-men/*.

awareness of or opportunities in critical areas including education, jobs, healthcare, housing, and credit.

B. NTIA Should Include Purpose Specification and Use Limitation Among Its List of Privacy Outcomes

Federal action on privacy should recognize baseline obligations that automatically attach when Americans' information is collected or used. The privacy outcomes enumerated in the RFC appear to move in this direction, but the Center on Privacy & Technology urges NTIA to consider also adding additional outcomes based on the familiar Fair Information Practices (FIPs) of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[11] The FIPs framework creates meaningful obligations for companies that collect personal data, and rights for individuals whose personal data is collected.

In particular, NTIA should add purpose specification and use limitation to the list of desired privacy outcomes. Entities that collect, share, and use Americans' data should be required to articulate the purpose for which they are engaging in collection or use, and to limit their activities—and the activities of any downstream or third-party actors—to uses that are consistent with that purpose.

IV. NTIA Should Recognize that Privacy Violations Themselves Are Harmful

In the RFC, NTIA notes the need to "minimiz[e] harm to individuals arising from the collection, storage, use, and sharing of their information."[12] In its description of the "reasonable minimization" privacy outcome, NTIA asserts that "data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm."[13] And in its list of high-level goals for Federal action, NTIA supports an approach to privacy regulations that is "based on risk modeling."[14] Taken together, these portions of the RFC could indicate that NTIA considers some privacy violations to be less harmful or even altogether harmless, and perhaps even that privacy violations that do not cause secondary harm need not be protected against.

The Center on Privacy & Technology urges NTIA to recognize that even when secondary harms are not immediately apparent, privacy violations are themselves harmful. The use of people's information in a way that exceeds social norms or user expectations violates user rights, undermines user trust, and contributes to an atmosphere of growing privacy concerns that ultimately may interfere with adoption and use of online services. For example, in 2016 NTIA found, based on data collected by the Census Bureau in 2015,

> Forty-five percent of online households reported that [privacy and security] concerns stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet, and 30 percent refrained from at least two of these activities.[15]

And in January 2016, the City of Portland, Oregon's Office for Community Technology reported that in focus groups conducted by the city to improve the city's understanding of adoption challenges, privacy concerns were raised in every group.[16]

In addition, even when privacy violations do not result in tangible and measurable harm to specific individuals, they may result in harms to society. For example, beyond subjecting individual users to specific uses and transfers that they find objectionable, information uses and misuses may harm society by:

- Supporting the dissemination of propaganda, misinformation, and disinformation. Americans' data may be used to generate and target false information, in-

---

[11] *See* Int'l Ass'n Privacy Professionals, *Fair Information Practices, https://iapp.org/resources/article/fair-information-practices/* (last visited Oct. 31, 2018); Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm* (last visited Oct. 7, 2018).

[12] RFC at 48601.

[13] *Id.*

[14] *Id.* at 480602.

[15] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities,* NTIA (May 13, 2016), *https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.*

[16] Angela Siefer, *Signs On Letter Encouraging FCC Protect Privacy Of Broadband Consumers,* NDIA (Jan. 26, 2016), *http://www.digitalinclusionalliance.org/blog/2016/1/26/ndia-signs-on-letter-encouraging-fcc-protect-privacy-of-broadband-consumers.*

cluding state-sponsored propaganda, careless or low-quality reporting, and false information designed and intended to undermine democracy.[17] As false information proliferates, Americans are rapidly losing trust in journalism.

- Amplifying hate speech. Americans' data may also be used to make the distribution of hateful and racist rhetoric and calls to violence more efficient.[18]
- Driving political polarization. Americans' data may also be used to drive content distribution platforms that are more likely to promote hyper-partisan content, which in turn may exacerbate political polarization. As one prominent legal scholar has written, "Self-insulation and personalization are solutions to some genuine problems, but they also spread falsehoods, and promote polarization and fragmentation."[19]
- Damaging public health. Digital sites and services often use users' data to inform design choices that will increase user engagement, including by intentionally designing products to be addictive and inescapable.[20] This can lead to a cascade of other problems, including heightened rates of depression, suicide, and sleep deprivation among young people.[21]

NTIA therefore should recognize that privacy violations must always be protected against, and should adopt caution as it considers any approach to privacy that conditions privacy obligations on the outcome of an assessment of risk of tangible secondary harms that individual users may suffer.

V. NTIA Should Not Support Regulatory "Harmonization" at the Expense of Context-Specific Privacy or of Strong Existing Protections

NTIA indicates that this Administration supports an approach to Federal action on privacy that prioritizes "harmoniz[ing] the regulatory landscape." The Center on Privacy & Technology urges NTIA not to support harmonization that comes at the expense either of context-specific privacy norms or of strong existing protections.

A. Protections for Americans' Private Information Should Take into Account the Context in Which Information Is Shared

There is no one-size-fits-all approach for privacy. Rather, privacy standards often must be context-specific, carefully tailored based on the avoidability of the information sharing, the sensitivity of the information share, and the expectations of consumers. As this Administration considers establishing comprehensive baseline privacy standards, existing laws should not be simultaneously eliminated. Many of those existing narrower privacy laws have already been appropriately tailored to establish heightened privacy standards under specific circumstances. These laws protect consumer information in specific contexts in which sharing is unavoidable—such as the information shared by students in an educational context,[22] by con-

---

[17] David McCabe, *Facebook Finds New Coordinated Political Disinformation Campaign,* Axios, July 31, 2018, *https://www.axios.com/facebook-finds-misinformation-campaign-4c5910b3-021a-45b7-b75c-b1ac80cbce49.html;* Dipayan Ghosh & Ben Scott, *Disinformation Is Becoming Unstoppable,* Time, Jan. 24, 2018; April Glaser & Will Oremus, *The Shape of Mis- and Disinformation,* Slate, July 26, 2018, *https://slate.com/technology/2018/07/claire-wardle-speaks-to-if-then-about-how-disinformation-spreads-on-social-media.html;* Alice Marwick & Rebecca Lewis, *Media Manipulation and Disinformation Online* (2017), *https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.*

[18] *See* Ariana Tobin, Madeleine Varner, & Julia Angwin, *Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up,* ProPublica, Dec. 28, 2017, *https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes;* Swathi Shanmugasundaram, Southern Poverty Law Center, *The Persistence of Anti-Muslim Hate on Facebook* (May 5, 2018), *https://www.splcenter.org/hatewatch/2018/05/05/persistence-anti-muslim-hate-facebook.*

[19] Cass R. Sunstein, #*Republic: Divided Democracy in the Age of Social Media* at 5 (2017).

[20] Center for Humane Technology, The Problem, *http://humanetech.com/problem/* (last visited Oct. 7, 2018) (explaining that operators of online services competing for users' attention are constantly learning how better to "hook" their users, and designing products intentionally to addict users).

[21] Recent studies have linked the use of platforms like Facebook, Snapchat, and Instagram to depressive symptoms in young adults caused by negatively comparing oneself to others on social media platforms. Brian A. Feinstein, *et al., Negative Social Comparison on Facebook and Depressive Symptoms: Rumination as a Mechanism,* 2 Psych. Pop. Media Culture 161 (2013). *http://psycnet.apa.org/record/2013-25137-002.* Experts have also found that teens who spend three hours a day or more on electronic devices are 35 percent more likely to have a risk factor for suicide and 28 percent more likely to get less than seven hours of sleep. Jean M. Twenge, *Have Smartphones Destroyed a Generation?,* The Atlantic, Sept. 2017, *https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198/.*

[22] Family Educational Rights and Privacy Act, 20 U.S.C. n§ 1232g.

sumers in a financial context,[23] by customers in a telecommunications context,[24] and by patients in a medical context.[25] This is also consistent with the FTC's evaluation of potentially problematic data-related practices under its Section 5 authority to prohibit unfair practices.[26]

Whether or not information sharing is avoidable by a consumer is often tied to the question of whether or not a service or transaction is essential. When a service is essential, information sharing may be considered unavoidable because the consumer cannot reasonably decline the service altogether. This, too, helps explain why heightened privacy protections apply in the educational,[27] financial,[28] telecommunications,[29] and medical contexts—all of these contexts involve essential services.[30]

B. New Protections for Americans' Privacy Should Not Eliminate Existing Protections

NTIA also should not support regulatory "harmonization" at the expense of existing protections that already benefit Americans under state or Federal laws. Americans are asking for *more* protections for their private information, not less. This is why Americans were outraged when Congress voted last year to eliminate strong privacy regulations that had been passed by the FCC.[31]

State laws play an important role in filling gaps that exist in Federal legislation. Consider, for example, the ways that states have expanded data security and breach notification laws over time to cover additional market sectors. Connecticut's data security and breach notification statute now covers entities operating at multiple nodes of the health care pipeline.[32] California adopted a data security statute—the Student Online Personal Information Protection Act (SOPIPA)—that is tailored to online educational platforms, and that prompted twenty-one other states to adopt student data security laws modeled on California's example.[33] Minnesota adopted a law requiring Internet Service Providers (ISPs) to maintain the security and privacy of consumers' private information.[34] And Texas now requires any nonprofit athletic or sports association to protect sensitive personal information.[35]

Some states have also expanded the types of information that data holders are responsible for protecting from unauthorized access, or for notifying consumers of when breached. For example, ten states have expanded breach notification laws so that companies are now required to notify consumers of unauthorized access to their biometric data—unique measurements of a person's body that can be used to determine a person's identity.[36] A large number of states also now require companies to notify consumers about breaches of medical or health data—information that can be used in aid of medical identity theft, potentially resulting in fraudulent healthcare charges and even introduction of false information into one's medical record.[37]

---

[23] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).

[24] 47 U.S.C. § 222.

[25] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).

[26] FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), *https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.*

[27] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

[28] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).

[29] 47 U.S.C. § 222.

[30] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).

[31] *See* Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular,* Vox, Apr. 4, 2017, *https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll.*

[32] C.G.S.A. § 38a-999b(a)(2) ("health insurer, health care center or other entity licensed to do health insurance business in this state, pharmacy benefits manager . . . third-party administrator . . . that administers health benefits, and utilization review company.").

[33] West's Ann.Cal.Bus. & Prof.Code § 22584(d)(1) (schools must "[i]mplement and maintain reasonable security procedures and practices. . .and protect that information from unauthorized access, destruction, use, modification, or disclosure."); Rachel Anderson, *Last Year's Education Data Privacy Legislation Trends,* iKeepSafe, Jan. 17, 2018, *https://ikeepsafe.org/last-years-education-data-privacy-legislation-trends/.*

[34] M.S.A. § 325M.05 (must "take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information.").

[35] V.T.C.A., Bus. & C. § 521.052 ("implement and maintain reasonable procedures. . .to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.").

[36] States that have done this include Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming.

[37] See Joshua Cohen, *Medical Identity Theft—The Crime that Can Kill You,* MLMIC Dateline (Spring 2015), available at *https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-*

Continued

And states are doing other important work on privacy as well. In addition to the California Consumer Privacy Act,[38] California also has a law requiring notification about breaches of information collected through an automated license plate recognition system.[39] Vermont has the Data Broker Act[40] and Illinois has the Biometric Information Protection Act.[41]

To avoid doing harm to consumers benefiting from these existing consumer protections, any Federal action on privacy or data security must preserve strong state standards. NTIA should, accordingly, approach calls for "harmonization" with caution.

VI. NTIA Should Identify Strong Privacy Enforcement Authority as a High-Level Goal for Federal Action

NTIA acknowledges that "[i]t is important to take steps to ensure that the FTC has the necessary resources" to enforce privacy. But more broadly, NTIA should clarify that what is needed is *strong* enforcement authority. Legislation should empower an expert agency or agencies to vigorously enforce the law—including the ability to fine companies for privacy and data security violations. The Federal Trade Commission does not have the ability to levy fines for privacy and data security.[42] This is widely viewed as a challenge by agency officials; indeed, civil penalty authority has been explicitly requested by multiple FTC officials, including Chairman Simons, Commissioner Slaughter, former commissioner Ohlhausen, former Commissioner Terrell McSweeny, and former director of the Bureau of Consumer Protection, Jessica Rich.[43] To improve privacy and data security for consumers, the FTC—or another agency or agencies—must be given more powerful regulatory tools and stronger enforcement authority.

The Center on Privacy & Technology agrees with NTIA that agencies also need resources to do their jobs well. The FTC is a relatively small agency, and should be given additional staff and resources if it is to be expected to step up its work on privacy. The agency would benefit from a larger Bureau of Technology equipped to fully grapple with the challenges of advancing technology—an idea supported by numerous current and former FTC officials.[44]

SE_Spring15.pdf ("A patient receiving medical care fraudulently can lead to the real patient receiving the wrong blood type, prescription, or even being misdiagnosed at a later time."). Medical or health data is covered by breach notification laws in Alabama, Arkansas, California, Delaware, Florida, Illinois, Kentucky, Maryland, Montana, Nevada, North Dakota, Oregon, Puerto Rico, Nevada, Rhode Island, Texas, Virginia, and Wyoming.

[38] California Consumer Privacy Act, *https://www.caprivacy.org/* (last visited October 7, 2018).

[39] West's Ann.Cal.Civ.Code § 1798.82(h).

[40] Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers,* TechCruch, May 27, 2018, *https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/*.

[41] 740 ILCS 14/1 et seq.

[42] There are exceptions to this rule. As the FTC explains, "If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule." FTC, *Privacy & Security Update 2016, https://www.ftc.gov/reports/privacy-data-security-update-2016.*

[43] *See, e.g., Oversight of the Federal Trade Commission: Hearing Before the Subcomm. On Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (calling for civil penalty authority, arguing that monetary penalties "would actually . . . cause the business to think through how it's conducting . . . its business and what it's doing in terms of security and privacy."); *id.* (statement of Rebecca Kelly Slaughter, Commissioner, Fed. Trade Comm'n) (calling for civil penalty authority); Maureen Ohlhausen, Commissioner, Fed. Trade Commission, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), transcript available at *https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf;* Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?,* 2 Geo. L. Tech. Rev. 514, 529 (2018), *https://www.georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-McSweeny-pp-514–30.pdf; Opportunities and Challenges in Advancing Health Information Technology: Hearing Before the Subcomms. On Info. Tech. and Health, Benefits, and Admin. Rules of the H. Oversight and Gov't Reform Comm.* (2016) (statement of Jessica Rich, Director of the Bureau of Consumer Protection, Fed. Trade Commission).

[44] A Bureau of Technology is an idea that has been cited by Chairman Joseph Simons, Commissioner Rebecca Kelly Slaughter, former Commissioner Terrell McSweeny, and Professor David Vladeck, former Director of the Bureau of Consumer Protection. *See, e.g.,* Oversight of the Federal Trade Commission: Hearing Before the Subcomm. On Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce (2018) (statement that the Commission is "affirmatively evaluating whether to create a bureau of technology"); McSweeny, *supra* note 4, at 530; U.S. Fed. Trade Comm'n, *Remarks of Commissioner Rebecca Kelly Slaughter on Raising the Standard: Bringing Security and Transparency to the Internet of Things?* at 5 (July

Even with additional staff and resources, however, enforcement agencies may, for a variety of reasons, sometimes fail to strongly enforce privacy standards.[45] To provide an additional backstop for consumers in the event that agencies lack the capacity or motivation to effectively enforce, Congress may also need to grant individual consumers themselves the right to bring civil actions against companies for violating privacy regulations.

State attorneys general should also be empowered to enforce privacy. A single agency cannot hope to police the entire digital ecosystem. State attorneys general do a large volume of important work in this area, both enforcing privacy laws and providing valuable guidance to companies trying to comply with the law. The guidance provided by state attorneys general is vitally important. Attorneys general frequently provide companies with ongoing guidance to help business understand, adapt to, and comply with legal requirements and best practices.[46]

State attorneys general will provide crucial complementary consumer protection support in thousands of small cases every year.[47] To ensure that consumers receive the best protection they possibly can, state attorneys general must be given the ability to help enforce any new Federal standard. This type of authority exists—and has been successful—under the Children's Online Privacy Protection Act.[48]

VII. NTIA Should Also Include Regulatory Agility Among Its High-Level Goals for Federal Action

Any new privacy and data security protection must also be designed to be forward-looking and flexible, with built-in mechanisms for updating standards in accordance with shifting threats. NTIA should acknowledge the importance of ensuring that digital era privacy protections are designed to express regulatory agility by including regulatory agility among its high-level goals for Federal action.

The need for regulatory agility is currently being met by state legislatures. In recent years, California passed the California Consumer Privacy Act[49] and Vermont

---

26, 2018), *https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter_-_raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf;* Aaron Fluitt, Institute for Technology Law & Policy at Georgetown Law, *Georgetown's David Vladeck Outlines Challenges and Opportunities for Incoming FTC Commissioners,* Apr. 6, 2018, *https://www.georgetowntech.org/news-fullposts/2018/4/7/april-6–2018-georgetowns-david-vladeck-outlines-challenges-opportunities-for-incoming-ftc-commissioners.*

[45] The FTC has come under criticism for not doing enough to enforce its consent decrees. *See* Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation,* Techonomy, May 4, 2018 *https://techonomy.com/2018/05/facebook-whatsapp-lesson-privacy-protection-necessary-innovation/.* And the FCC has been widely criticized for not doing enough to protect security and privacy of phone users. *See* Craig Timberg, *How Spies Can Use Your Cellphone to Find You–and Eavesdrop on Your Calls and Texts, Too,* Wash. Post, May 30, 2018, *https://www.washingtonpost.com/business/technology/how-spies-can-use-your-cellphone-to-find-you—and-eavesdrop-on-your-calls-and-texts-too/2018/05/30/246bb794-5ec2-11e8-a4a4-c070ef53f315_story.html; Wyden Demand FCC Investigate Unauthorized Tracking of Americans' Cell Phones,* May 11, 2018, *https://www.wyden.senate.gov/news/press-releases/wyden-demands-fcc-investigate-unauthorized-location-tracking-of-americans-cell-phones;* Violet Blue, *FCC Shrugs at Fake Cell Towers Around the White House,* Endgaget, June 8, 2018, *https://www.engadget.com/2018/06/08/fcc-shrugs-at-fake-cell-towers-around-the-white-house/.*

[46] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General,* 92 Notre Dame L. Rev. 747, 759 (2016); Paul Shukovsky, *State Attorneys General Are Crucial Force in Enforcement of Data Breach Statutes,* Bloomberg Law: Privacy & Data Security, Oct. 7, 2013, *https://www.bna.com/state-attorneys-general-n17179877665/.*

[47] For example, according to the Massachusetts State Attorney General's Office, Massachusetts alone saw 2,314 data breaches reported in 2013, 97 percent of which involved fewer than 10,000 affected individuals. *Discussion Draft of H.R., Data Security and Breach Notification Act of 2015: Hearing Before the Subcomm. On Commerce, Manufacturing, and Trade of the H. Energy & Commerce Comm.* (2015) (statement of Sara Cable, Assistant Att'y Gen. Office of Mass. State Att'y Gen.). Each data breach affected, on average, 74 individuals. *Id.*

[48] The Children's Online Privacy Protection Act enables state attorneys general to bring actions on behalf of residents of their states against operators of online sites or services that they believe have violated children's privacy regulations. 15 U.S.C. §6504. State attorneys general use this authority; indeed, just weeks ago, the State Attorney General of New Mexico filed a suit against several companies for alleged children's privacy violations. *See AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data* (Sept. 12, 2018), *https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location_Personal_Data_1.pdf.*

[49] California Consumer Privacy Act, https://www.caprivacy.org/(last visited November 1, 2018).

passed the Data Broker Act.[50] Between 2015 and 2018 at least 23 states—from all regions of the country—passed data security or breach notification legislation.[51]

Given the high level of legislative activity currently taking place at the state level on these issues, the most straightforward way that Federal action on privacy can preserve regulatory agility in privacy and data security would be simply by leaving state legislative authority intact. In the event, however, that Federal action on privacy seeks to resolve differences between state laws by establishing a uniform Federal standard, it must ensure that robust mechanisms for regulatory agility are built in. One such mechanism would be robust rulemaking authority for any agency or agencies that are to be tasked with protecting the privacy and security of Americans' information. Indeed, FTC commissioners have directly asked Congress for rulemaking authority.[52] Rulemaking enables agencies to adjust regulations as technology changes, as the FTC did just a few years ago with the COPPA Rule.[53]

VIII. Conclusion

NTIA's proposed approach to consumer privacy offers a number of positive elements. The Center on Privacy & Technology urges NTIA to move further in the direction of strong consumer protection by recognizing additional important privacy outcomes and high-level goals for Federal action, and by approaching calls for a risk-based approach and harmonization with caution.

Respectfully submitted,

LAURA M. MOY,
GABRIELLE REJOUIS,
Center on Privacy & Technology,
Georgetown Law.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JERRY MORAN TO NUALA O'CONNOR

Question. Your testimony described concerns with the resources available to the FTC to effectively enforce consumer privacy under its current Section 5 authorities. As a member of the Senate Appropriations Subcommittee with jurisdiction over the FTC, I am particularly interested in understanding the resource needs of the agency based on its current authorities, particularly before providing additional authorities. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

---

[50] Devin Coldeway, *Vermont Passes First Law to Crack down on Data Brokers,* TechCrunch, May 27, 2018, *https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/*.

[51] Since 2015, data security or breach notification legislation has been enacted in Alabama, Arizona, California, Connecticut, Delaware, Florida, Illinois, Iowa, Maryland, Montana, Nebraska, New Hampshire, New Mexico, North Dakota, Oregon, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, and Wyoming. *See* Nat'l Conf. State Legislatures, *2015 Security Breach Legislation* (Dec. 31, 2015), *http://www.ncsl.org/research/telecommunicatons-and-information-technology/2015-security-breach-legislation.aspx;* Nat'l Conf. State Legislatures, *2016 Security Breach Legislation* (Nov. 29, 2016), *http://www.ncsl.org/research/telecommunicatons-and-information-technology/2016-security-breach-legislation.aspx;* Nat'l Conf. State Legislatures, *2017 Security Breach Legislation* (Dec. 29, 2017), *http://www.ncsl.org/research/telecommunicatons-and-information-technology/2017-security-breach-legislation.aspx;* Nat'l Conf. State Legislatures, *2018 Security Breach Legislation, http://www.ncsl.org/research/telecommunicatons-and-information-technology/2016-security-breach-legislation.aspx* (last visited Nov. 1, 2018).

[52] Maureen K. Ohlhausen, FTC Commissioner, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), available at *https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf* ("Legislation in both areas—data security and breach notification—should give the FTC . . . rulemaking authority under the Administrative Procedure Act"); *Oversight of the Federal Trade Commission: Hearing Before the Subcomm. On Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (stating he "support[s] data security legislation that would give the authority to issue implementing rules under the Administrative Procedure Act"); *id.* (statement of Rebecca Kelly Slaughter, Comm'r) (calling for APA rulemaking authority); *id.* (statement of Rohit Chopra, Comm'r) (also supporting rulemaking authority, stating, "the development of rules is a much more participatory process than individual enforcement actions and it also gives clear notice to the marketplace rather than being surprised, and I think it would be a good idea.").

[53] Federal Trade Commission, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Amending Children's Online Privacy Protection Rule,* Dec. 19, 2012, https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

Answer. The FTC needs more staff to carry out the agency's privacy and data security enforcement mission. CDT's draft privacy legislation includes the following provisions to add personnel to the bureau of consumer protection:

(1) IN GENERAL.—Notwithstanding any other provision of law, the Director of the Bureau of Consumer Protection of the Commission shall appoint—(A)100 additional personnel in the Division of Privacy and Identity Protection of the Bureau of Consumer Protection, of which no fewer than 25 personnel will be added to the Office of Technology Research and Investigation; and no fewer than 25 additional personnel in the Division of Enforcement of the Bureau of Consumer Protection.

(2) AUTHORIZATION OF APPROPRIATIONS.—There is to be authorized to be appropriated to the Director of the Bureau of Consumer Protection such sums as may be necessary to carry out this section.

Because additional resources may only lead to an increase in the number of FTC enforcement actions and not a change in the type of cases brought, we recommend new baseline privacy standards and original fining authority. CDT's draft legislation proposes such amendments and can be found at *https://cdt.org/campaign/federal-privacy-legislation/*.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO NUALA O'CONNOR

Question 1. In both the EU's GDPR and California's Consumer Privacy Act, parental consent is necessary for collection and processing of children's personal data. Is parental consent an effective model for protecting children?

Answer. Parents should be empowered to make meaningful decisions about how children use technology and how information collected about them is used. While parental consent requirements have an appropriate role to play in ensuring this, we should recognize that privacy laws like the GDPR stress that consent should be freely given, specific, and informed. It is not clear that generalized consent obligations can achieve this command. Extensive "notice and choice" mandates do not provide individuals with meaningful control over their data,[5] and this extends to parents' ability to effectively manage the privacy of their children.[6]

Assuming parental consent is either effective or appropriate, it is also important to understand what exactly parents are being asked to consent to. For example, the Children's Online Privacy Protection Act, which is the primary U.S. Federal law that governs privacy rights for children, requires consent merely for the collection of children's personal information. While this appears to be broadly protective, it results in parents being asked to consent to data collection without sufficient knowledge or effective controls over how that information is then used. Establishing clear prohibitions around intrusive and unfair data collection and use is needed to better protect children, but this requires policymakers to make difficult choices about what types of data use to take off the table. An unwillingness to make this choice is why privacy frameworks shift this decision onto individuals and parents through a "notice and choice" model.

The GDPR and California Consumer Privacy Act (CCPA) address this somewhat by placing restrictions on how information can be used. For instance, the GDPR requires risk assessments and places obligations on companies for any use of personal data. The CCPA specifically requires parental consent before personal information about children may be sold. Placing prohibitions or restrictions on uses of information can better address exploitative data practices.

Question 2. A recent *New York Times* analysis found that both the Apple App Store and the Google Play Store have apps in their respective children's or family sections that potentially violate Children's Online Privacy Act (COPPA).[7] What specific role should platform owners play to ensure compliance on their platforms?

Answer. It is apparent that the structure and scale of platforms have brought into question whether COPPA compliance is sufficient. CDT believes there are a number

---

[5] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review 1880 (2013).

[6] Steven Johnson, The Bargain at the Heart of the Kid Internet, The Atlantic (April 12, 2018), *https://www.theatlantic.com/family/archive/2018/04/child-data-privacy/557840/*.

[7] Valentino-DeVries, J., Singer, N., Krolick, A., Keller, M. H., "How Game Apps That Captivate Kids Have Been Collecting Their Data." *The New York Times.* 2018, September 12. *https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html*

of measures that platforms could voluntary engage in to address this problem.[8] Platforms can better alert third-party apps and services to their specific obligations to obtain consent and protect children's information. For example, at present, the Apple App Store Review Guidelines references COPPA only once under a brief discussion of legal requirements around children.[9] The Google Play Store Developer Center presents more information to developers.[10] Providing guidance and further COPPA compliance resources for smaller app developers could be useful, as well.

Platforms could also make it easier to flag apps that present privacy issues. A mechanism for receiving complaints when combined with the existing types of automatic analysis and review undertaken by app stores could help surface trends with respect to COPPA compliance. With this information, platforms could consider voluntarily reporting alleged COPPA violations to the FTC and being more transparent with respect to enforcement of their own developer terms. A longstanding issue with self-regulation is the lack of clear insight into what should or does happen when a company violates those terms.[11]

Violation of developer terms may also raise regulatory ire. The FTC has held companies liable under Section 5 of the FTC Act for misleading statements that are made to other businesses, particularly if those representations impact consumers, raising tough questions about business-to-business contracts and developer terms of services.[12]

Question 3. It seems hard to achieve compliance if the large tech platforms have no responsibility or liability for apps they are hosting, especially when these apps can be put there by fly-by-night operators overseas who do not care if they are in violation of U.S. law. What rules and enforcement should the U.S. have in place to ensure that the big tech platforms are properly protecting children's privacy?

Answer. Platforms play a vital role as gatekeepers to apps, services, and features that impact the privacy of children. However, COPPA does not require platforms either to vet or monitor third-party applications that may be directed to children or to otherwise comply with COPPA on behalf of any third-party application. While platforms allow individuals to directly connect with other entities that may have independent COPPA obligations, app stores do not make any decisions about what content or services individuals ultimately interact with. Platforms generally operate as neutral intermediaries that facilitate the ability of developers to create and upload applications and individuals to select the content of their choice. Under Section 230 of the Telecommunications Act, 47 USC § 230, such intermediaries are not liable for content they do not author. Similarly, primary responsibility for COPPA compliance should lie with the party directing its services to children, and not the platform that facilitates this connection.

CDT does not support extending liability under COPPA to platforms. However, we do believe the Federal Trade Commission ought to investigate COPPA compliance across the app ecosystem and explore the efficacy of platforms' voluntary efforts. We are concerned that the FTC is not using its existing investigatory and enforcement authorities under COPPA, and we believe Congress may wish to encourage the FTC to be more proactive in its enforcement posture.

Question 4. Since COPPA was enacted, the FTC has only brought 28 COPPA cases with over 10 million in civil penalties, what changes should be made to the legislation or the regulation to ensure more vigorous enforcement?

Answer. At least from what is conveyed externally, proactive enforcement of COPPA from the FTC appears to be lacking. For instance, in its first children's privacy case involving internet-connected toys, the FTC settled with VTech for $650,000 for collecting the personal information of hundreds of thousands of children without providing direct notice to parents or obtaining verifiable parental consent.[13] These violations were only discovered, however, after a public data breach involving the electronic toy manufacturer.

---

[8] Alethea Lange & Emma Llanso, A Closer Look at the Legality of "Ethnic Affinity", Center for Democracy & Tech. (Nov. 7, 2016), *https://cdt.org/blog/a-closer-look-at-the-legality-of-ethnic-affinity/*.

[9] *https://developer.apple.com/app-store/review/guidelines/#kids*

[10] *https://play.google.com/about/families/coppa-compliance/*

[11] Joseph Jerome, Uber's Fingerprinting Foibles and the Costs of Not Complying with Industry Self-Regulation, Center for Democracy & Tech. (April 26, 2017), *https://cdt.org/blog/ubers-fingerprinting-foibles-and-the-costs-of-not-complying-with-industry-self-regulation/*.

[12] See *https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.*

[13] FTC Press release, January 8, 2018, *https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated*

CDT acknowledges that the FTC has limited resources, but proactive investigations and enforcement actions prior to blatant privacy violations are essential to ensure COPPA's protections keep pace with evolving technologies. Further, raising awareness around enforcement actions is important as it gives guidance about what are considered unacceptable practices and deters other companies from taking similar actions. This is true both inside and outside of the FTC. For example, improving communications and outreach by making the COPPA Safe Harbor annual reports to the FTC, which have descriptions of all disciplinary actions taken by the Safe Harbor programs, public by default, so other companies are deterred from committing future violations.

More recently, we should not discount the important role that state Attorneys General can play in ensuring more vigorous enforcement of COPPA. However, if more evidence can be brought forward to suggest systemic underenforcement, Congress might explore providing parents with a private right of action to enforce substantive provisions in COPPA.

Question 5. Do you think the COPPA Safe Harbor program is effective in ensuring that children's privacy is protected? Why or Why not?

Answer. The FTC has, to date, approved seven Safe Harbor organizations[14], which enable industry groups and other organizations to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final rule. There has been significant criticism of how the Safe Harbor process operates, including low industry participation and a general lack of transparency.[15] Absent more public transparency into who participates, how program operators identify and remediate issues, and what resources the FTC places in oversight, it is difficult to be certain how effective these programs are. A good way to do this, as mentioned before, would be to make public the annual reports that the Safe Harbors send to the FTC, which have descriptions of all disciplinary actions taken by the Safe Harbor programs, to better understand the impact of Safe Harbors in protecting children's privacy.

CDT generally recommends that the FTC provide ongoing monitoring, training, and evaluation to ensure these Safe Harbors are effectively enforcing COPPA and applying the same enforcement rigor entrusted to the FTC. For example, while the FTC may take an enforcement action after any violation of COPPA, Safe Harbor organizations may be much more accommodating of bad practices, attempting to remediate multiple violations before referring companies to the FTC.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MAGGIE HASSAN TO NUALA O'CONNOR

Question. Ms. O'Connor, you wrote in your testimony about notice and consent fatigue and expressed your frustrations with the fact that the model of relying on consumers' consent to lengthy, legalistic privacy notices persists "despite the fact that few individuals have the time to read [these notices], and it is difficult, if not impossible, to understand what they say even if they are read." You suggested that we could improve on this model by setting in place baseline levels of privacy protections that might mitigate the need for lengthy and complex notice and consent provisions. Would you be able to elaborate for us how we might address this issue of notice and consent fatigue and what some of those baseline protections might be?

Answer. The way to address notice and consent fatigue is to shift the burden of protecting privacy away from individual consumers. This requires setting baseline limits on how entities can process personal information. Baseline privacy protections should (1) grant access, correction, deletion and portability rights to users, (2) require reasonable security practices and transparency from companies, (3) prevent advertising discrimination against protected classes, and (4) presumptively prohibit certain collection and use of sensitive data for secondary purposes. These protections must be enforced by a fully-staffed and resourced FTC, as well as state attorneys general.

If Congress only addresses numbers 1 and 2 above, individuals will still be left with the burden of deciphering an endless stream of notices and attempting to make choices that align with their privacy interests. Even if it were possible to read and understand each privacy notice, the ultimate privacy risk from any individual consumer data transaction is impossible to forecast. For example, imagine the choice to sign up for a customer loyalty card, which many people would consider a mun-

---

[14] COPPA safe harbor program, *https://www.ftc.gov/safe-harbor-program*

[15] Brandon Golob, How Safe are Safe Harbors? The Difficulties of Self-Regulatory Children's Online Privacy Protection Act Programs (2015).

dane act. To make a truly informed privacy choice, one would have to consider all of the items she might buy over the course of many years—over-the-counter medication, food, clothing—and how that information might be used by any number of entities, including insurers and healthcare providers, to make decisions affecting her healthcare, the pricing of items targeted to her, and her priority when she calls customer service. Under a notice and consent regime, even the shrewdest and most privacy conscious customers will inevitably lose control over their sensitive personal data. To truly rebalance the consumer-corporate data relationship and protect digital civil rights, legislation must address the secondary and the discriminatory use of data through systemic changes in corporate behavior.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO NUALA O'CONNOR

Question 1. Selling Versus Leveraging Data: Facebook, Google, and other companies with similar business models do not sell data, but rather they leverage data to sell advertisements. An advertiser approaches an edge provider with an audience it would like to reach and the edge provider uses the data it maintains to match the ad to the desired audience. The fact that the data do not change hands is immaterial for consumers' experience, but it still is a distinction that various laws treat differently. I think when we talk about giving consumers notice about how data is used, intricacies like this can be difficult to explain in the context of a notice and consent model. How should we think about this distinction?

Answer. CDT agrees that privacy interests can be implicated even if data does not leave the possession of the company that originally collected it. Indeed, the difference between selling and leveraging data may be meaningless to consumers who are rightfully concerned about the aggregation and use of their sensitive information to target them with ads and other content. There are two ways to address this. The first is to ensure that notice includes a description of how information will be used and on whose behalf, even if it does not technically change hands. This will not only address the advertising model you mention above, but instances where a single company operates across verticals or different online services. Many companies would argue they already do this to some extent, but it is apparent that the intricacies of online advertising are lost on even the most technically-sophisticated online users.

The second, better approach is to ensure that legislation goes beyond transparency to create baseline privacy rights that consumers can expect from all covered entities. We recommend that Congress pass legislation that grants individual rights to access, correct, delete and port data. We also recommend that the legislation create a presumption that certain secondary uses of sensitive data including precise geolocation, biometrics, children's information is unfair. These overarching rights will ensure that the vagaries of corporate ownership do not frustrating meaningful privacy protections.

Question 2. Privacy Enhancing Technology: The major theme of this debate has been how technology has changed the relationship between the consumer and their expectation of privacy. In general, we have talked about how technology can enable more and better information for consumers while at the same time jeopardizing their privacy. But at the same time, technology can also enhance privacy. Encryption, anti-virus, cybersecurity technologies are all examples of this. How do you think we can help develop these technologies at the Federal level?

Answer. Beyond passing baseline privacy legislation, the Federal government should use its procurement power to ensure that the products and services it purchases include privacy and security controls. This will not only protect government systems, but also likely send more privacy and security-friendly products into the consumer market.

While the Federal Government has long set contracting standards on privacy and security, it has issued extensive data and product management guidance over the last several years which could improve the next generation of government purchases. Documents drafted or updated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) now clearly delineate agency obligations and provide technical advice on how to incorporate privacy controls into products.[16] The executive and legislative branches could do more

[16] OMB Circular A–130 (2016), NISTIR 8062 (2017), NIST 800–63, Rev. 5, (2018),

to speed the adoption of such products either through legislative mandates [17] or better funding current IT modernization efforts.[18]

Question 3. Federal Preemption: Technology companies make the argument that one single, national standard would make the most sense in the United States because a patchwork of 50 different laws would not work to regulate something as fluid as data. Are there any circumstances under which you would be in support of Federal preemption of state privacy laws?

Answer. CDT agrees that there are benefits to creating a single Federal privacy standard for personal data: predictability for consumers and companies, consistency across jurisdictions, and providing privacy rights to all U.S. citizens in a reasonable time period.

However, denying states the right to defend their residents' privacy interests on their own terms is a serious decision. Congress should only preempt state laws in return for meaningful privacy protections and a serious enforcement structure. As we discuss in more detail in our written statement, we believe legislation should, 1) grant access, correction, deletion and portability rights to users, 2) require reasonable security practices and transparency from companies, 3) prevent advertising discrimination against protected classes, 4) presumptively prohibit certain collection and use of sensitive data for secondary purposes, and 5) grant considerable resources to the FTC and empower state attorneys general to enforce the law. While FTC APA rulemaking is not necessary to effect all of these recommendations, it would be particularly helpful in delineating reasonable security standards, enforcing traditional civil rights laws in the online world, and determining what process would be appropriate for covered entities to seek approval to repurpose sensitive data.

We look forward to working with Congress to ensure preemption language is appropriate in scope. Avoiding unintended consequences is more complicated than it appears on first blush. Most states have laws regulating the use of personal information outside of the consumer context covered by this bill and should be left intact.[19]

Question 4. Data Protection Officers: As you well know under Europe's GDPR there is a requirement that any entity that handles large amounts of data appoint a Data Protection Officer, or DPO. DPOs are responsible for educating the company on compliance, training staff in data processing, providing advice on data protection, and so on. What is your perspective on this requirement?

Answer. CDT believes that requiring an employee to be tasked with and be accountable for a company's privacy and security decisions can be beneficial but is ultimately a process requirement. Process requirements in and of themselves benefit the largest actors while guaranteeing nothing to consumers. Any legislation should prioritize clear delineations about what data processing behavior is required of covered entities.

Question 5. Notice and Consent: The notice and consent model, while helpful, is not a silver bullet. Consumers are likely to click through and face decision fatigue about the many different privacy policies on every different platform. From your perspective, what data practices, if any, should be prohibited in general?

Answer. CDT believes that it is appropriate and timely for Congress to flip the privacy presumption and declare a limited set of data practices unfair. The nexus between secondary uses—those which aren't related to the service or product a consumer or user signed up for—and sensitive data is the ideal place to start. We recommend prohibiting most secondary uses of precise geolocation, biometrics, and health information, and limiting the disclosure or repurposing of other types of data, such as private communications and data captured by microphones and cameras on consumer devices.

For example, this would mean that precise geolocation information provided to operate a mapping service could not be repurposed for precise location-based advertising. CDT believes that these secondary use limits align with consumers' expectations. These general prohibitions should be subject to a safety valve whereby the FTC could exempt certain secondary uses where the benefits to consumers or the

---

[17] See for example S. 1691, The Internet of Things (IoT) Cybersecurity Improvement Act of 2017, introduced by Senator Mark Warner (D-Va.).

[18] The Technology Modernization Fund was created by congress in 2018 and controls $100 million dedicated to updating government systems under a more streamlined contracting process. An estimated $85 billion was spent last Fiscal Year on information technology, which overwhelming is used to maintain legacy systems. See *https://itdashboard.gov/*.

[19] Take for example, criminal laws prohibiting identity fraud, stalking or revenge porn, state level Privacy Acts to protect government held personal information, individual torts and civil cases, or local industry regulations for transportation, safety, or other non-privacy purposes.

public clearly outweigh the privacy risks and appropriate safeguards and controls are in place.

○