S. HRG. 115–893

EXAMINING SAFEGUARDS FOR CONSUMER DATA PRIVACY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 26, 2018

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
58–443 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

EXAMINING SAFEGUARDS FOR CONSUMER DATA PRIVACY

WEDNESDAY, SEPTEMBER 26, 2018

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

The Committee met, pursuant to notice, at 10 a.m. in room SDG–50, Dirksen Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Nelson, Wicker, Fischer, Klobuchar, Moran, Schatz, Tester, Cortez Masto, Lee, Peters, Hassan, Blumenthal, Markey, Udall, Gardner, and Cruz.

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

The CHAIRMAN. Good morning. A decade from now we may look back and view this past year as a watershed with respect to the issue of consumer data privacy.

A year ago this month, news of the massive Equifax data breach made the headlines. Shortly thereafter, we brought the company's then current and former CEOs before the Committee for a public accounting.

Then in April, the Commerce Committee and Judiciary Committee held a joint hearing with Facebook CEO, Mark Zuckerberg, after revelations that political intelligence firm, Cambridge Analytica, had acquired access to the personal data of millions of unwilling Facebook users.

In May, the European Union's General Data Protection Regulation, known as GDPR, took effect with many privacy-related mandates and severe penalties for violators.

In June, the Consumer Protection Subcommittee held a hearing entitled "Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks," where Aleksandr Kogan, the Cambridge University academic at the center of the Cambridge Analytica controversy, testified.

On June 28, the California Consumer Privacy Act was signed into law. Like GDPR, the new California law, which will take effect on January 1, 2020, contains many privacy mandates and severe penalties for violators.

These developments have all combined to put the issue of consumer data privacy squarely on Congress's doorstep. The question is no longer whether we need a Federal law to protect consumers' privacy. The question is what shape will that law take?

To examine the impact of all of these developments, we're pleased to be joined today by representatives of some of the leading technology companies and Internet service providers in America.

There's often a temptation to lump industry leaders like these together as if they were all the same, but as we'll hear today, they actually have very different approaches to the collection, use, and protection of consumer data.

I expect the witnesses to offer candid testimony about how their companies seek to address privacy concerns about their products and services and how new privacy requirements impact them.

I want to hear how they are complying or planning to comply with GDPR and the California Consumer Privacy Act, the advantages and disadvantages of both laws from their perspectives, and the steps they believe the Federal Government should take to help protect consumer privacy.

I hasten to add that this will not be the only hearing on consumer data privacy we will hold. Some have expressed angst that we have an industry-only panel here today. Let me reassure anyone who thinks we're going to be rushing through legislation without the benefit of alternative views that things don't work that way here.

Early next month, we intend to convene a second hearing that will include privacy advocates as well as other key stakeholders.

Alastair Mactaggart, the California privacy activist, and Andrea Jelinek, the Head of GDPR Enforcement for the European Union, have agreed to attend.

It's also important to remember that while we have not enacted a comprehensive national data privacy law, concern about privacy is not a new issue for Congress. Over the past 20 years, Congress has enacted laws in privacy affecting particular segments of the population and sectors of the Nation's economy, such as the Children's Online Privacy Protection Act, the Health Insurance Portability Act, and the Gramm-Leach-Bliley Act.

But now we've arrived at a moment where I believe there's a strong desire by both Republicans and Democrats and by both industry and public interest groups to work in good faith to reach a consensus on a national consumer data privacy law that will help consumers, promote innovation, reward organizations with little to hide and force shady practitioners to clean up their act.

While this hearing grows out of recent concerns about consumer privacy, it's not intended to be a gotcha hearing. Instead, it represents the beginning of an effort to inform our development of a Federal privacy law that enjoys strong bipartisan support.

Politics is always about timing and I believe now is the time to begin action on this important issue.

I look forward to working with colleagues on both sides of the aisle in the coming months.

And with that, I'll recognize the Ranking Member, Senator Nelson, for his opening statement.

Senator Nelson.

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

Senator NELSON. Thank you, Mr. Chairman, and as you noted, this is not the first hearing on the privacy issue. We've had many hearings because consumers have been hit by the misuse of their personal information and by data breaches all over the place. Consumers are worried: Do they have any privacy anymore?

We have a number of witnesses here that will hopefully provide the Committee with valuable insight into how their companies safeguard their customers' private information.

So let's get on with the hearing.

[The prepared statement of Senator Nelson follows:]

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

Thank you, Mr. Chairman, for holding a hearing on this critical issue. This is not the committee's first hearing on data privacy—in fact, the committee has held many hearings on this issue throughout the years because consumers have been hit by the misuse of their personal information and by data breaches left and right.

We have a number of witnesses here with us today who will hopefully provide this committee with valuable insight into how their companies safeguard their customers' private information.

With that, Mr. Chairman, and for the sake of time, I will go ahead and turn it over to our witnesses.

We look forward to hearing from you all.

The CHAIRMAN. Thank you, Senator Nelson. Very succinct. I like that.

Well, we do have a big panel today, and we look forward to hearing from them and having members of the panel have the opportunity to ask questions and interact. So we will get started.

And with us today, we have Mr. Len Cali, who's Senior Vice President for Global Public Policy at AT&T; Mr. Andrew DeVore, who's the Vice President and Associate General Counsel at Amazon.com, Inc.; Mr. Keith Enright, who's the Chief Privacy Officer at Google; Mr. Damien Kieran, who is the Global Data Protection Officer and Associate Legal Director at Twitter, Inc.; Mr. Guy "Bud" Tribble, Vice President for Software Technology at Apple, Inc.; and Ms. Rachel Welch, who is the Senior Vice President for Policy and External Affairs at Charter Communications, Inc.

So we welcome you all here, appreciate your willingness to join us today, and obviously look forward to hearing from you.

We'll ask you, if you can, to keep your oral remarks to 5 minutes or thereabouts, and your entire statements will be included as a part of the permanent record.

But we'll start on my left and your right with you, Mr. Cali, so nice to have you here. Please proceed.

STATEMENT OF LEONARD CALI, SENIOR VICE PRESIDENT, GLOBAL PUBLIC POLICY, AT&T, INC.

Mr. CALI. Thank you, Chairman Thune, Ranking Member Nelson, and members of the Committee.

As noted, my name is Len Cali. I'm with AT&T, responsible for Global Public Policy.

AT&T has a 140-year heritage of innovation that includes eight Nobel Prizes and 15,000 patents and pending patents worldwide.

We employ nearly 220,000 Americans, representing every state, and over the past 5 years, we've invested $135 billion in the United States, more than any other public company. Without doubt, we are deeply invested in our country, our communities, our employees, and our customers.

AT&T is committed to protecting our customers' privacy and securing their information. We provide notice of our practices, we give consumers choices about how their data is used, and we protect their data. We believe in transparency.

AT&T welcomes today's conversation. We believe it is important for Congress to weigh in on the issue of privacy and provide consumers and business clear national rules concerning how consumer information is used, shared, and protected, regardless of the company that collects it.

We are not newcomers to this position and now there appears to be growing agreement about the need for a new and comprehensive Federal privacy law. We thank this committee for its important work on this issue.

The task before Congress is complex; namely, how to protect and empower consumers concerning their personal information and privacy while at the same time not impeding the innovation and consumer benefits that flow from responsible use of data.

There are important consumer interests on both sides of the question. My written testimony suggests some privacy principles for this Committee to consider, though, in the end, the decision on how to strike the right balance is appropriately yours.

Let me begin with three basic points. First, collection of information is today widespread. It happens when you walk in a retail store, search the Internet, visit a social media site, drive your car and buy your groceries. It also happens on millions of apps, games, and websites where technology running in the background captures what you are accessing, reading, and viewing.

Internet access companies, like AT&T, also collect information, though to a lesser extent than you might expect. Encryption of data between the mobile device and the website masks more than 80 percent of the Internet traffic coming through AT&T's access facilities.

Second, there are different types of information to consider. Some is provided directly by the consumer, some is observed by a company, and some is inferred based on analysis of still other information.

With each type, some information is sensitive, something that a consumer considers private, and some is not. Different consumers may draw the line in different places.

Third, different uses of the same type of information may offer consumers entirely different benefits and raise different risks.

For instance, a wireless company cannot complete a call without knowing your physical location. The information is sensitive but essential to the service. When location information is publicly posted for military personnel by a fitness tracker, however, that's a different matter. It may be a problem. But if personal identifiers are removed, location information could enhance a beneficial traffic mapping app and, of course, the use of data-driven advertising

powers many of the free, relevant, and discounted services that American consumers enjoy every day.

These points highlight the complexity of the challenge. The solution in contracts should be straightforward and uniform. Consumers need understandable rules of the road, regardless of the company collecting their data or the technology used.

In addition, to preserve the benefits of responsible data use, restrictions should be risk-based, turning on the sensitivity and use of the data.

The rules also should give consumers the ability to choose how their information is treated. This is similar to the current FTC Framework. It's a good framework but it can be improved.

Consumers and business would be better served by greater clarity around the types and uses of data that require heightened levels of consumer consent.

It is also important to establish a single Federal framework. It will confuse customers and be unworkable for businesses of every kind to comply with multiple state rules when offering anything that relies on customer data.

There are many issues to discuss, but I'm confident common ground can be found. AT&T looks forward to working with Congress and other stakeholders to establish a nationwide set of privacy protections that provide consumers strong and uniform safeguards that foster innovation and competition and that confirm the FTC as the nation's privacy regulator.

Thank you for having me here. I look forward to your questions.

[The prepared statement of Mr. Cali follows:]

PREPARED STATEMENT OF LEONARD CALI, SENIOR VICE PRESIDENT, GLOBAL PUBLIC POLICY, AT&T

Thank you Chairman Thune, Ranking Member Nelson, and Members of the Committee.

I am Leonard Cali, Senior Vice President Global Public Policy for AT&T. AT&T has a 140-year heritage of innovation that includes eight Nobel Prizes and 15,000 patents and pending patents worldwide. We employ nearly 220,000 Americans, representing all 50 states. Over the past five years we've invested $135 billion in the United States, more than any other public company. Without doubt, we are deeply invested in our country, our communities, our employees and our customers.

Protecting our customers' privacy is a fundamental commitment at AT&T, and we understand the great responsibility that comes along with our customers' trust in allowing AT&T to collect and use their data. On behalf of AT&T, I thank you for this opportunity to participate in the critical discussion concerning the future of U.S. privacy regulation.

While we've all been talking about privacy for years, today we stand at a critical juncture in that discussion. Perhaps for the first time, there is widespread agreement among industry, policy makers and many consumer groups of the need for a new and comprehensive Federal privacy law. This consensus is driven by a recognition that in today's data-driven world, it is more important than ever to maintain consumers' trust and give them control over their personal information. Consumers rightly expect that consistent privacy protections will apply regardless of which app, device, service or company is collecting and using their personal information.

However, there is an increasing risk that we will end up with a patchwork quilt of inconsistent privacy regulations at the Federal and state level, which will only serve to confuse consumers and stifle innovation. And there is a risk that regulators will fail to strike the right balance in addressing privacy by importing the European Union's overly regulatory privacy regime.

Now is the time for decisive Congressional leadership to establish a thoughtful and balanced national privacy framework. AT&T strongly supports Federal privacy legislation that both protects consumers and allows for innovation. Such legislation would not only ensure that consumer privacy rights are protected, but it would also

provide consistent rules of the road across competing websites, content, devices and applications.

Of course, there are differing views on what should be in a national privacy law. We expect that, and we will actively participate in discussions to reach consensus on a forward-looking framework. Fortunately, there is an emerging, wide-spread (and growing) consensus around basic privacy principles that should be the starting point for Federal legislation.

Specifically, there is growing consensus that policy makers should design a national privacy law that builds upon the FTC's successful privacy framework and that:

- *Establishes consistent nationwide privacy protections for consumers.* Privacy protections should be based on the sensitivity and use of consumers' information, not by the type of entity collecting it. Legislation should preempt state privacy laws and provide consumers one set of consistent privacy protections, choices and controls.
- *Avoids duplication and inconsistent requirements.* To accomplish this, the Federal privacy law can be overseen exclusively by the FTC, an agency with decades of experience regulating privacy practices.
- *Respects customer privacy choices, requiring companies to be transparent about their privacy practices.* Legislation should require companies to have a privacy policy that gives consumers clear and comprehensible information about the categories of data that are being collected, how consumer data is used and the types of third parties with whom data may be shared. Customers should have easy-to-understand privacy choices. Legislation should define sensitive and non-sensitive data and its appropriate treatment (*e.g.,* opt-in/out) consistent with the FTC's established framework.
- *Allows innovative, consumer-friendly uses of data that enhance their lives, subject to appropriate protections.* Strong privacy protections and innovation are not mutually exclusive goals. Legislation should affirmatively allow innovative uses of data, subject to effective safeguards. Consumers benefit from data-driven innovations that deliver high-quality services, reduce their costs, enhance their lives, and develop new, improved products.
- *Requires companies to take reasonable steps to protect consumer data.* Data security and breach-notification legislation should establish a reasonable, flexible and consistent national framework.
- *Supports collaborative public-private partnerships.* Voluntary privacy programs and standards developed through public-private collaboration could serve as a safe harbor in legislation while enabling companies to adapt to rapidly changing technology and market developments. In particular, we welcome the Administration's efforts, though NTIA, to work with stakeholders to establish a set of privacy principles that would provide an alternative to the European Union's prescriptive approach and be used in Federal legislation.

AT&T is actively engaged with industry, consumer stakeholders and policymakers to build agreement around these principles, and we look forward to working with Congress to pass privacy legislation around them.

AT&T's Commitment to Customer Privacy

Protecting our customers' privacy and securing their information is a fundamental commitment at AT&T. Like you, we believe that consumers deserve strong privacy and security protections that give them control over how their information is used and shared, as well as confidence that their information will be protected.

We believe that customers should have choices and control about how their information is used by AT&T and shared with other companies. This includes opting in or out of some programs, setting privacy preferences, and unsubscribing from marketing e-mails and letters.

We keep customers' information safe using encryption or other appropriate security controls. All of our employees are subject to the AT&T Code of Business Conduct (COBC) and certain state-mandated codes of conduct. Under the COBC, all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of our customers' records. We take this seriously. Any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action, including dismissal.

To the extent AT&T has records in its custody or control that are subject to a mandatory legal obligation to produce the records, AT&T will comply with that legal

requirement. We ensure that government requests are valid, and that our responses comply with the law and our own policies. Although we comply with legitimate government requests for customer communications, we do so only to the extent required by law.

In addition, since 2014, AT&T has issued a Transparency Report that identifies the number and types of legal demands for customer information received in criminal, civil, and national security matters, as well as emergency situations. It also includes international demands related to global operations for customer information and website blocking. The Transparency Report is available in Spanish, to better inform our Mexican and Latin American customers.

AT&T is dedicated to being a leader in protecting customer privacy and providing our customers security, transparency, respect, choice and control.

The Need for Federal Privacy Legislation

For decades, the FTC's privacy regime has provided a predictable and technology neutral approach to privacy that focuses on customer transparency and consumer choice. The FTC's privacy framework has provided customers strong privacy protections, while allowing companies flexibility to innovate. By choosing this framework, as opposed to prescriptive requirements, the FTC has been able to keep pace with rapidly evolving technology and markets. Overly prescriptive prohibitions, in contrast, can limit the consumer benefits that come from innovation.

The FTC has also been an aggressive cop on the beat. It has brought more than 500 enforcement actions for privacy and data security violations, including cases involving major Internet and telecommunications companies.

As you know, in May 2018, the European Union's General Data Protection Regulation (GDPR) went into effect.[1] Some argued that the United States and other countries should quickly import GDPR. One month later, in June 2018, California enacted its Consumer Privacy Act of 2018 (AB 375), which applies to companies doing business in California. While the California law is different in many respects from GDPR, like GDPR, it applies its requirements to essentially all companies that collect data. We support uniform application of the law.

However, also like GDPR, many of the California requirements are highly prescriptive, and ambiguities and errors in its language leave open serious questions about how it will be enforced and interpreted.[2] For both the California law and GDPR, there also remain serious questions about their ultimate impact on consumers, desirable new technologies like AI, and the marketplace.

But I am not here to provide Congress a laundry list of the possible negative implications of the California law. The more important point for Congress and this Committee to understand is that the passage of the California law and interest of other states in legislation raise the imminent risk that companies and consumers will soon face a patchwork of inconsistent state privacy laws. Indeed, twenty-six state privacy bills were introduced this year alone, and the passage of the California law will no doubt stimulate more state legislative action. Some states may follow the more-regulatory California/GDPR route, while other states may adopt a more flexible approach, similar to the FTC's framework. Regardless, what is certain is that future state privacy laws will differ in significant ways.

A patchwork of differing state privacy law will confuse consumers, providing them uneven protections and potentially forcing them to navigate a complicated menu of diverging state-specific privacy choices and controls. Imagine a customer trying to understand why she might be required to opt in to a particular privacy setting in Maryland, while being required to opt out of that setting in Virginia. Or why certain data is subject to heightened protections in Florida, but not South Dakota. And in a world where more and more communications and commerce occur on mobile devices, will legal requirements be determined by locations of those devices at any given time, the telephone numbers or IP addresses assigned to those devices, or the principal residences of the owners of those devices? While consumer protections often vary by state in our Federal system, these variations make less sense when data moves freely, without regard to state borders and at the speed of a light. Consumers deserve a single set of privacy rules that they can understand and rely upon across the Nation.

---

[1] On the one hand, GDPR is a consistent framework, applicable to all companies that collect and use European sensitive data. On the other hand, it is still very much an open question how GDPR will be interpreted and enforced by European regulators. Even though AT&T does not offer consumer-facing services in Europe, we have spent significant time and resources ensuring our compliance with GDPR, having enhanced our documentation, procedures and technologies to ensure our compliance, where required.

[2] In particular, the law grants the state Attorney General broad rulemaking authority.

Further, while each state may adopt its own set of privacy permissions and restrictions, providers struggling with compliance may have no choice but to adopt the most restrictive elements of each state's law, given the impracticability of complying with multiple state rules when offering mobile and Internet services that, by their nature, have no state boundaries. The result may be a more restrictive privacy framework than any state intended with less innovation, investment and consumer welfare than any state anticipated.

Differing privacy laws also raise business compliance costs. For example, compliance with the California law will require extensive changes to customer-facing policies and privacy controls, as well as internal systems and business processes. These challenges and resulting costs would be exponentially greater were states to adopt laws with different requirements.

As states adopt privacy laws that clash with the FTC's long-standing framework, the FTC's position as the Nation's leading privacy regulator will inevitably be eroded. In short, Federal legislation is necessary to codify a privacy law that builds on and strengthens the FTC's role as the Nation's preeminent privacy "cop on the beat."

Conclusion

AT&T looks forward to working with this Committee and Congress to establish a nationwide set of privacy protections that, consistent with the principles outlined above, provide consumers with strong and uniform safeguards and strengthen the FTC's position as the Nation's leading privacy regulator.

The CHAIRMAN. Thank you, Mr. Cali.

Mr. DeVore.

STATEMENT OF ANDREW DEVORE, VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL, AMAZON.COM, INC.

Mr. DEVORE. Good morning. Thank you, Chairman Thune, Ranking Member Nelson, and members of the Committee.

I'm Andrew DeVore, Vice President and Associate General Counsel at Amazon.

Amazon's mission is to be Earth's most customer-centric company. Our corporate philosophy is firmly rooted in working backward from what customers want and continuous innovation to provide customers better service, greater selection and lower prices. We apply this approach across all areas of our business, including those that touch on consumer privacy.

Customer trust is our highest priority. We've known from our very beginning as an online bookstore that we must get privacy right in order to meet customers' high expectations.

Many core features of the Amazon experience, including foundational shopping features, like showing what other customers bought and product recommendations, depend on us using customer data responsibly and transparently.

Our customer-centric approach has made privacy by design principles a core feature of our business since our founding. We design our products and services so that it's easy for customers to understand when their data is being collected and controlled when it's shared.

Our customers trust us to handle their data carefully and sensibly, in a secure and appropriate manner in line with their expectations, and we're not in the business of selling our customers' personal data.

From this vantage point, we have four policy perspectives for the Committee's consideration.

First, to ensure that we all share in the benefits of technology with confidence that customer data is being handled responsibly

and transparently, legislation addressing privacy issues should be carefully crafted in a process that involves all relevant stakeholders.

Built on a foundation as a retailer and our long-standing commitment to privacy and data security, we know data privacy issues are complex and touch every sector of the economy.

Second, we encourage Congress to ensure that additional overhead and administrative demands that any privacy legislation might require actually produce commensurate privacy benefits.

Our longstanding commitment to privacy aligned, as well, with the principles of the European Union's General Data Protection Regulation. Meeting its specific requirements for the handling, retention, and deletion of personal data required us to divert significant resources to administrative tasks and away from invention on behalf of customers.

Third, Amazon supports the goals of the California Consumer Privacy Act of giving consumers visibility and control when businesses collect and sell their personal information, but Congress should consider possible unintended consequences of the CCPA approach.

Because the CCPA was enacted so quickly there was little opportunity for thoughtful review, resulting in some provisions that ultimately do not promote best privacy practices.

Finally, while creating smart privacy policies and practices takes careful attention, we believe that strong focus on the customer makes it easier to make good decisions.

When you start with the customer and work backward, the correct answer is often right in front of you. We share the goal of finding common solutions, particularly in times of fast-moving innovation. As technology evolves, so, too, will opportunities for all of us in this room to work together. We look forward to those opportunities.

Thank you and I look forward to your questions.

[The prepared statement of Mr. DeVore follows:]

PREPARED STATEMENT OF ANDREW DEVORE, VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL, AMAZON.COM, INC.

Thank you, Chairman Thune, Ranking Member Nelson, and Members of the Committee.

I am Andrew DeVore, Vice President and Associate General Counsel at Amazon. Amazon's mission is to be Earth's most customer-centric company. Our corporate philosophy is firmly rooted in working backwards from what customers want and continuous innovation to provide customers better service, more selection, and lower prices. We apply this approach across all areas of our business, including those that touch on consumer privacy.

Amazon's Approach to Privacy

Customer trust is our highest priority—we know we must get privacy right in order to meet our customers' high expectations. Many core features of the Amazon experience—including foundational shopping features like showing what other customers bought and product recommendations—depend on us using customer data responsibly and transparently. Understanding what products customers like and how customers use our services helps us make better recommendations, improve our products and services, and invent new products and services that will delight our customers.

While compliance with applicable laws provides a baseline for our privacy decisions, our foremost concern when considering privacy issues is customer trust. We have known from our very beginnings as an online bookstore that maintaining cus-

tomer trust is essential to our success. Our customers trust us to handle their data carefully and sensibly in a secure and appropriate manner in line with their expectations. Any privacy mistake risks the loss of that trust and serious reputational damage even if there is no violation of privacy laws.

Our customer-centric approach has led Amazon to follow privacy by design principles since our founding. We design our products and services so that it is easy for customers to understand when their data is being collected and control when their data is shared. And we are not in the business of selling our customers' personal data.

Two examples—Product Recommendations and Amazon Echo—help highlight how, by working backwards from the customer, Amazon gets privacy issues right and builds products and services that earn customer trust. Product recommendations, which help customers discover items they might otherwise not have found, are core to the Amazon shopping experience. Customers see these features in clearly labeled formats like "Frequently bought together" and "Customers who viewed this item also viewed." We use aggregate data from our customers' browsing and purchase behavior in order to make recommendations, such as suggesting baby wipes and tear-free shampoo for a customer purchasing diapers.

In a vacuum, this might sound concerning—"Amazon is tracking what customers search and purchase." But because product recommendations are clearly labeled, intuitive to customers, and provide a valuable service, customers love them. Customers are not surprised that we collect and use data in this way. That is one of our goals—while our terms of use of course describe the collection of this data, we don't want customers to feel they need to read our terms to avoid being surprised. As product recommendations illustrates, we strive to make our data collection practices intuitive and transparent for customers by tying them directly to the shopping and discovery experience.

Alexa is a cloud-based voice service that lets customers play music, ask questions, make calls, send and receive messages, and get information, news, sports scores, and weather, among other things. On our Echo family of devices, customers speak to Alexa by saying the "wake word" (Alexa, Amazon, Echo, or Computer). So, from across a room, customers can say, "Alexa, play music," "Alexa, what's the weather forecast for tomorrow," or "Alexa, turn on the living room lights," and get an immediate response, with no need to use their hands or look at a screen.

With the Echo, Amazon invented a brand new category of devices totally unfamiliar to customers. So we knew we had to get privacy right to preserve our customers' trust. From early-stage development, we built privacy deeply into the Echo hardware and Alexa service by design, and we put customers in control.

As a result, we designed the wake word to function as an audible "on button" for Echo devices. Echo devices detect the wake word by using on-device keyword spotting technology that identifies acoustic patterns that match the wake word. No audio is sent to Amazon unless either the device detects the wake word or Alexa is activated by pressing the action button present on some Echo devices.

Once Alexa is activated, Echo gives customers clear notice it is streaming audio to the cloud. For instance, the light ring on Echo will turn blue or a blue bar will appear on Echo Show, an Echo device with a screen. Customers can also configure Echo devices to play a short audible tone to indicate the device has recognized the wake word and is streaming audio to the cloud. We also employ additional technical measures to minimize the amount of audio and background noise streamed to the cloud, and we give customers control of their recordings, including the ability to see and play back each recording associated with their account and delete those voice recordings one-by-one or all at once.

We also include an additional physical control for customers—a microphone off button that electrically disconnects the Echo device's microphones, combined with a dedicated red light confirming the microphones are off. As an additional safeguard, we designed the circuitry of Echo devices so that power can only be provided either to that dedicated red light or to the device microphones, not to both at the same time. So when the dedicated red light is on, customers know the microphones are off and no audio can be recorded and streamed to the cloud.

These multiple layers of privacy controls for Alexa and our Echo family of devices are a result of our privacy by design process, which incorporates privacy considerations into every stage of product development.

Policy Viewpoints

Our customer obsession leads us to four perspectives for the Committee's consideration as you consider a Federal approach to privacy and specifically the effect of the California Consumer Privacy Act of 2018 (CCPA) and the European Union General Data Protection Regulation (GDPR).

First, built on our foundation as a retailer and our longstanding commitment to privacy and data security, we know data privacy issues are complex and greatly impact every sector of the economy. Legislation addressing these issues should be carefully crafted in a process that involves all the relevant stakeholders to ensure that we all share the benefits of technology with confidence that our data is being handled responsibly and transparently.

Second, while our long-standing commitment to privacy aligned us well with the GDPR principles, meeting its specific requirements for the handling, retention, and deletion of personal data required us to divert significant resources to administrative and record-keeping tasks and away from inventing new features for customers and our core mission of providing better service, more selection, and lower prices. We encourage Congress to ensure that additional overhead and administrative demands any legislation might require, actually produce commensurate consumer privacy benefits.

Third, Congress should consider possible unintended consequences of the CCPA approach. Amazon supports the CCPA's goals of giving consumers visibility and control when businesses collect and sell their personal information. But because the CCPA was quickly enacted there was little opportunity for thoughtful review, resulting in some provisions that ultimately do not promote best practices in privacy. For example, CCPA's definition of "personal information" goes beyond information that actually identifies a person to include any information that "could be linked with a person," which arguably is all information. The result is a law that is not only confusing and difficult to comply with, but that may actually undermine important privacy-protective practices like encouraging companies to handle data in a way that is not directly linked to a consumer's identity.

Finally, creating smart privacy policies and practices takes careful attention, and a strong focus on the customer makes it easier to make good decisions. When you start with the customer and work backwards, the correct answer is often right in front of you. Technology is an important part of modern life, and has the potential to offer extraordinary benefits we are just beginning to realize. Customers should know how their data is being used and be empowered to make their own individual determination of the benefits they gain from choosing to use new services and technologies. We believe that policymakers and companies like Amazon have very similar goals—protecting consumer trust and promoting new technologies. We share the goal of finding common solutions, especially during times of fast moving innovation. As technology evolves, so too will the opportunities for all of us in this room to work together.

Thank you, and I look forward to your questions.

The CHAIRMAN. Thank you, Mr. DeVore.

Mr. Enright.

STATEMENT OF KEITH ENRIGHT, CHIEF PRIVACY OFFICER, GOOGLE

Mr. ENRIGHT. Chairman Thune, Ranking Member Nelson, and members of the Committee, thank you for the opportunity to speak here today.

I appreciate your leadership and I welcome the opportunity to discuss Google's work on privacy and security.

My name is Keith Enright, and I am Google's Chief Privacy Officer. I lead Google's Global Privacy Legal Team and together with Product and Engineering partners direct our Office of Privacy and Data Protection.

Across every economic sector, government function, and organizational mission, data and technology are critical keys to success. At Google, we combine data with cutting-edge technology to build products and services that improve people's lives, help grow the economy, and make the Web safer.

With partners, we are working to tackle big challenges and enable scientific breakthroughs. All this relies on the collection and use of data with strong privacy and security practices.

As the world becomes increasingly data-focused, there is rightly increased focus on the impacts on consumers and whether there should be better rules of the road for data privacy.

We understand that this committee may be legislating on privacy and we support that effort. We are looking forward to constructively engaging with you to help protect consumers, improve the ecosystem, and encourage continued investment in innovation.

To that end, just this week, we put forward principles for a responsible data framework which we hope will be a helpful contribution to this committee's work.

I briefly want to cover four key issues that we believe are critical elements to this discussion: transparency, control, portability, and security.

First, transparency. Google's approach to privacy stems directly from our founding mission to organize the world's information and make it universally accessible and useful. Providing most of our products for free is a key part of being that mission and ads help make that happen.

With advertising, as with all of our products, users expect us to keep their personal information confidential and under their control. We do not sell personal information. This is important and I want to repeat that point. We do not sell personal information.

We acknowledge that we have made mistakes in the past from which we've learned and improved our privacy program. We understand that the foundation of our business is trust. To maintain that trust, we must clearly explain how our products use personal information and provide easy-to-find user-friendly controls to manage privacy.

We strive to be upfront about the data we collect, why we collect it, and how we use it. This starts with ensuring that our privacy policy is clear and concise and making privacy controls immediately accessible from the privacy policy.

We look for ways to add transparency into our products directly so that users can understand the privacy implications of their choices right in context from how you share documents in Google Drive to why you are seeing certain ads.

Second, with regard to greater user control, our privacy tools are built for everyone. Different people have different ideas about privacy, so we must build with that in mind.

For users who have a Google account, we put these privacy and security settings in a single place, Google Account, to make it easy to set their preferences.

I want to call attention to our security checkup and privacy checkup tools, which respectively help users identify and control apps which have access to their Google account data and guide users to review and change their security and privacy settings, like deleting their Google activity, disabling personalized ads, or downloading a copy of their information.

Third, we believe data portability is a key way to drive innovation, facilitate competition, and best serve our users. That's why we've been working on it for over a decade.

If a user wants to try out or even switch to another product or service, they should be able to do so as easily as possible, not be locked into a service. That's why just this year, we announced the

Data Transfer Project which we developed and are now working on with partners and industry.

Fourth, security considerations are paramount in all of these efforts. Securing the infrastructure that provides Google services is critical in light of the growing and sophisticated nature of many threats directed at our services and our users.

All Google products are built at their core with strong security protections, including continuous efforts to block a range of security threats.

We also work to help users improve their own cyber security. For example, we have offered two-step verification to our users since 2011.

Our focus on security is not limited to Google's users. We share technologies and collaborate with partners. One example is our free and publicly available Safe Browsing Tool, which helps protect users from phishing and malware.

I want to conclude by saying that more than any other time in my career in privacy, there is momentum toward codifying baseline privacy requirements in law. We welcome this. A healthy data ecosystem requires that people feel comfortable that all entities who process personal information will be held accountable for protecting it.

Privacy and security work is never finished. Our work will continue and we stand ready to do our part to help build a better ecosystem for everyone.

Thank you again for the opportunity to be here today. We look forward to continuing our work with you on these important issues and I welcome any questions you might have.

[The prepared statement of Mr. Enright follows:]

PREPARED STATEMENT OF KEITH ENRIGHT, CHIEF PRIVACY OFFICER, GOOGLE

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee: thank you for the opportunity to appear before you this morning. I appreciate your leadership on the important issues of data privacy and security, and I welcome the opportunity to discuss Google's work in these areas.

My name is Keith Enright, and I am the Chief Privacy Officer for Google. I have worked at the intersection of technology, privacy, and the law for nearly 20 years, including as the functional privacy lead for two other companies prior to joining Google in 2011. In that time, I have been fortunate to engage with legislators, regulatory agencies, academics, and civil society to help inform and improve privacy protections for individuals around the world.

I lead Google's global privacy legal team and, together with product and engineering partners, direct our Office of Privacy and Data Protection, which is responsible for legal compliance, the application of our privacy principles, and generally meeting our users' expectations of privacy. This work is the effort of a large cross-functional team of engineers, researchers, and other experts whose principal mission is protecting the privacy of our users.

Across every single economic sector, government function, and organizational mission, data and technology are critical keys to success. With advances in artificial intelligence and machine learning, data-based research and services will continue to drive economic development and social progress in the years to come. Doctors use data to save lives; farmers rely on data to increase yields; and charities analyze data to better serve our communities. I have had the privilege of working with government agencies to better leverage data to advance their mission and provide improved care and benefits to Americans efficiently and reliably. Businesses of all types and sizes, far beyond those represented at this hearing today, collect and use data. In my previous experience, I saw first-hand the transformative efforts by traditional brick and mortar retail businesses to improve efficiency, reduce costs, and delight consumers through the innovative use of data.

At Google, we combine cutting-edge technology with data to build products and services that improve people's lives and enhance their productivity, help grow the economy,[1] improve accessibility[2] and make the web safer and more secure.[3] With partners, we are working to tackle big societal challenges and enable medical[4] and scientific breakthroughs.[5] These types of benefits all rely on the collection and use of data, and must come with, and not at the expense of, privacy and security.

Privacy That Works For Everyone

We acknowledge that we have made mistakes in the past, from which we have learned, and improved our robust privacy program.

The foundation of our business is the trust of people that use our services. To maintain user trust, we must clearly explain how our products use personal information, and to provide easy-to-find and use controls to manage privacy. We also invest in research and development of cutting-edge privacy and security engineering techniques, sharing what we learn to benefit the broader ecosystem.

Google's approach to privacy stems directly from our founding mission: to organize the world's information and make it universally accessible and useful. Providing most of our products for free is a key part of meeting that mission, and ads help us make that happen. With advertising, as with all our products, users trust us to keep their personal information confidential and under their control. We do not sell personal information. Period.

As the world becomes increasingly data-focused, there is, rightly, increased focus on the impacts on consumers and whether there should be better rules of the road for data privacy. We understand that Congress may be legislating on privacy and we support that effort. We look forward to constructively engaging with you as your work develops.

To that end, I want to briefly cover four key issues that we believe are critical elements to this discussion: transparency, control, data portability, and security. These components are also central to Google's recently released framework for responsible data protection regulation, which I will discuss as well.

Informing Users And Explaining Our Practices

First, transparency is a core value of our approach to serving users. Google strives to be upfront about the data we collect, why we collect it, and how we use it. We get that privacy policies are not users' first choice in reading material, but we work to make ours clear and concise. Outside experts have praised ours as best in class.[6] Just this year we updated our Privacy Policy to be easier to understand, with informative videos that explain our practices and settings. In addition to making our privacy controls easy to find in user accounts and through Google Search, we have also made them immediately accessible from the Privacy Policy so that users can make decisions about their account settings as they learn about our practices.

We also look for ways to add transparency into our products directly, so that users can understand the privacy implications of their choices in context. For example, if you add a Google Drive file to a shared folder, we'll check to make sure you intend to share that file with everyone who has access to that folder. With Why This Ad,[7]

---

[1] Last year, Google's tools helped provide $283 billion of economic activity in the U.S. for more than 1.5 million businesses, website publishers, and nonprofits nationwide (*https://economicimpact.google.com/*).

[2] For example, we have used data analysis and machine learning to enable closed captioning on over 1 billion YouTube videos in 10 languages making them accessible to the over 300 million deaf or hard of hearing people around the world (*https://youtube.googleblog.com/2017/02/one-billion-captioned-videos.html*).

[3] Google Safe Browsing (*https://safebrowsing.google.com*) helps protect over three billion devices every day, and it is free and publicly available for developers and other companies to use.

[4] Working with physicians and other healthcare experts, we've developed systems that can detect diabetic eye disease (*https://ai.googleblog.com/2016/11/deep-learning-for-detection-of-diabetic.html*) and breast cancer tumors (*https://ai.googleblog.com/2018/02/assessing-cardiovascular-risk-factors.html*), help predict medical outcomes (*https://ai.googleblog.com/2018/05/deep-learning-for-electronic-health.html*), and even shed light on connections between cardiovascular disease and images of the eye (*https://ai.googleblog.com/2018/02/assessing-cardiovascular-risk-factors.html*).

[5] We've shown machine learning can help predict molecular properties, which could aid everything from pharmaceuticals to photovoltaics to basic science (*https://ai.googleblog.com/2017/04/predicting-properties-of-molecules-with.html*). Another example is that Google's AI technology helped discover the first 8-planet system outside our own (*https://www.blog.google/technology/ai/hunting-planets-machine-learning/*).

[6] Time Magazine and the Center for Plain Language ranked Google number one among technology companies for best privacy policy (*http://time.com/3986016/google-facebook-twitter-privacy-policies/*).

[7] *https://support.google.com/ads/answer/1634057?hl=en*

you are able to click or tap on an icon in each ad to find out why you are seeing that particular ad and understand more about how Google's system makes these decisions. Another example is if someone wants to install a new app on their Android mobile phone, they can see the types of personal information that apps can access right on the screen before deciding whether to install it. If they change their mind or want to learn more, they can learn about the different permissions, and disable specific ones. Finally, our Transparency Report [8] provides information to the public on how government actions can affect the free flow of information online. We are always working to expand the information we provide to users.

Google Account Controls

Second, with regard to user control, our privacy tools are built for everyone. Different people have different preferences about how they want their information to be used, and preferences can vary over time, so we build products and controls that do not presume all users are the same. For instance, a Search user can choose not to sign in when they search, and a Chrome user can choose to use Chrome's Incognito mode. For users who have a Google account, we put their privacy and security settings in a single place—Google Account [9]—so users don't have to visit several different apps or pages to see their data and set their preferences for how Google should store and use their information.

Google was one of the first companies to offer users this type of centralized dashboard [10] in 2009, and we continue to develop and improve these and other tools to make them more robust and intuitive. These efforts are working: in 2017, nearly 2 billion people visited their Google Account controls.[11]

I particularly want to call attention to our Security Checkup [12] and Privacy Checkup [13] tools, which respectively, help users identify and control the apps that have access to their Google account data, and guide users to review and change their security and privacy settings. These checkups help users make decisions about what information they are sharing, who they are sharing it with, and what to expect when they share it. It is not enough to just have these tools available: we actively encourage users to do privacy and security reviews by reminding them to use these tools through service-wide promotions and individual prompts.

Google Account is where users can:

- download a copy of their personal information;
- see or delete their Google activity, such as search queries or browsing, by date, product, or topic;
- disable personalized ads or see the information Google uses to personalize their ads; and
- locate a lost or stolen phone.

Privacy From The Ground Up

Protecting users is about more than just being transparent and offering control—it requires building products that reflect our privacy commitments and principles at every stage of their development. Doing this properly requires a comprehensive data protection program that includes privacy design reviews, engineers dedicated to privacy to review code and data flows, and a system to manage and address any issues discovered before users are put at risk. Google has had such a program for over seven years, and we continue to expand and refine it.

Data Portability

Third, we believe data portability is a key way to drive innovation, facilitate competition, and best serve our users—that's why we have been working on it for over a decade.[14]

---

[8] *https://transparencyreport.google.com/?hl=en*

[9] *https://myaccount.google.com/intro?hl=en-US*

[10] Dashboards are a recognized best practice (*https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf*).

[11] See: *https://www.blog.google/technology/safety-security/improving-our-privacy-controls-new-google-dashboard/*, *https://www.blog.google/technology/safety-security/celebrating-my-accounts-first-birthday/*, and *https://googleblog.blogspot.com/2015/06/privacy-security-tools-improvements.html* for more information.

[12] *https://myaccount.google.com/security-checkup*

[13] *https://myaccount.google.com/privacycheckup?otzr=1*

[14] *https://publicpolicy.googleblog.com/2009/09/introducing-dataliberationorg-liberate.html*

Google has always believed that people should use our products because they provide unique value and features. Download Your Data [15] is a practical tool that lets users backup or archive important information, organize information between multiple accounts, recover from account hijacking, and explore the data stored in their account.

Currently, users average around one million exports per month covering eight billion files. We enable export from more than 50 Google products, even offering the option to import data directly into our competitors' systems. If a user wants to try out a new product or service or even switch because they think it is better, they should be able to do so as easily as possible, not be locked into an existing service.

Portability is one way we ensure that users can trust Google with their data. This is why we led the development of the Data Transfer Project,[16] an open-source platform that enables you to move a copy of your data directly from one account to another without downloading and reuploading. For people who rely on phones and mobile networks for connectivity, this is a tremendous improvement. We're grateful for our industry partners' contributions to this project, and look forward to working with others.

Security

Fourth, security considerations are paramount in all of these efforts. The security threat landscape that we see is increasingly complex and wide ranging. Securing the infrastructure that provides Google's services is critical in light of the growing and sophisticated nature of many threats directed at our services and users.

All Google products are built with strong security protections at their core to continuously and automatically detect threats and protect users. We devote significant resources to fortify Google's infrastructure and this includes continuous and proactive efforts to identify and block a wide range of security risks. The insights we've gained serving billions of people around the world help us stay ahead.

We have also worked to help our users improve their own cybersecurity posture. For example, we have offered two-step verification to our users since 2011,[17] and last year, we unveiled the Advanced Protection Program,[18] which provides the strongest account protection that Google offers.

Our focus on security is not limited to Google's users. We share technologies and collaborate with partners to help people stay safer whenever they are online. In 2007, we launched the first version of our Safe Browsing tool.[19] This tool helps protect users from phishing, malware, and other potential attacks by examining billions of URLs, software, and website content. We have made Safe Browsing free and publicly available to webmasters and developers so that they can protect their websites and applications from malicious actors.

Finally, it is important to note that small and midsize businesses are leveraging Google's cloud technology to protect the security and confidentiality of their business data. In the past, many such businesses managed their own online security infrastructure, putting them at a disadvantage. Now, these small and midsize businesses can avail themselves of the security expertise previously only available to the largest, most sophisticated enterprises, significantly reducing their information technology costs while vastly improving the security, confidentiality, integrity, and availability of business critical data.

Toward A Comprehensive Baseline Privacy Framework

Now, more than any time I've seen in my career in privacy, there is an interest in setting out baseline privacy requirements in law. We welcome this: a healthy data ecosystem requires people feel comfortable that all entities who use personal information will be held accountable for protecting it.[20]

The U.S. approach to privacy is admirable for its focus on protecting consumers while encouraging innovation and investment, but there is room for improvement. To demonstrate our commitment to the goal of comprehensive baseline privacy legislation, we recently put forward principles for a responsible data framework. The framework is based on the Fair Information Practices Principles (FIPPs), OECD Privacy Principles, Asia-Pacific Economic Cooperation (APEC) Privacy Framework, as-

---

[15] *https://support.google.com/accounts/answer/3024190?hl=en*

[16] See website (*https://datatransferproject.dev/*) and white paper (*https://datatransferproject.dev/dtp-overview.pdf*) for more information.

[17] *https://www.google.com/landing/2step/*

[18] *https://google.com/advancedprotection/*

[19] *https://safebrowsing.google.com/*

[20] Comments filed in U.S. Department of Commerce, Docket No. 100402174–0175–01 and Docket No. 101214614–0614–01: Information Privacy and Innovation in the Internet Economy (2010).

pects of the European General Data Protection Regulation (GDPR), and our 20 years of experience offering services that depend on information, privacy protections, and user trust. It includes many of the principles I have talked about today: transparency, control, data portability, and security.

I am submitting a copy of Google's framework with my testimony. We hope it can contribute to this Committee's work.

Our framework is high-level, and of course, the manner in which general principles are implemented will matter a great deal. We urge the Committee to take into consideration the impacts on service functionality, the consumer benefits of free and low-cost products, the future of the open web and app ecosystem, the unique compliance needs of new entrants and small businesses, and competitive market dynamics.

Conclusion

Privacy and security work is never finished. Our work will continue, and we stand ready to do our part in building a better ecosystem for everyone. Sound practices and smart regulations can help, particularly when they are applied across the board to those making decisions regarding the collection and use of personal data. We share your goals of ensuring consumers are protected and businesses have an opportunity to innovate and grow.

Thank you again for the opportunity to tell you about our continued efforts in this space. We look forward to continuing to work with Congress on these important issues. I welcome any questions you might have.

ATTACHMENT

FRAMEWORK FOR RESPONSIBLE DATA PROTECTION REGULATION

In our digital era, a growing array of organizations use personal data to provide a growing range of services. Responsible data use can unlock benefits for people, companies, and other organizations around the world. Regulation can protect individuals and communities from harm and misuse of data, and help maintain the trust that enables innovation and change. Building on our efforts to provide innovative services that rely on personal data, and on our experience with evolving international privacy laws, we have synthesized the following set of high-level principles. These principles are based on established privacy regimes and are meant to apply to organizations that make decisions regarding the collection and use of personal information. This framework helps Google evaluate legal proposals and advocate for smart, interoperable, and adaptable data protection regulations.

Requirements

Collect and use personal information responsibly.

Organizations must operate with respect for individuals' interests when they process personal information. They must also take responsibility for using data in a way that provides value to individuals and society and minimizes the risk of harm based on the use of personal information (*i.e.,* data that can be linked to a person or personal device).

Mandate transparency and help individuals be informed.

Organizations must be transparent about the types of personal information they collect, why they collect it, and how they use or disclose it, particularly when used to make decisions about the individual. Regulators should encourage organizations to actively inform individuals about data use in the context of the services themselves, helping to make the information relevant and actionable for individuals.

Place reasonable limitations on the manner and means of collecting, using, and disclosing personal information.

Collection and use of personal information can create beneficial and innovative services, within a framework of appropriate limits to the collection, use, and disclosure of personal information to ensure processing occurs in a manner compatible with individuals' interests and social benefits.

Maintain the quality of personal information.

Organizations should make reasonable efforts to keep personal information accurate, complete, and up-to-date to the extent relevant for the purposes for which it is maintained. Data access and correction tools, as mentioned below, can assist organizations in meeting this obligation.

Make it practical for individuals to control the use of personal information.

Organizations must provide appropriate mechanisms for individual control, including the opportunity to object to data processing where feasible in the context of the service. This does not require a specific consent or toggle for every use of data; in many cases, the processing of personal information is necessary to simply operate a service. Similarly, requiring individuals to control every aspect of data processing can create a complex experience that diverts attention from the most important controls without corresponding benefits.

Give individuals the ability to access, correct, delete and download personal information about them.

Individuals must have access to personal information they have provided to an organization, and where practical, have that information corrected, deleted, and made available for export in a machine-readable format. This not only empowers individuals, it also keeps the market innovative, competitive, and open to new entrants.

Include requirements to secure personal information.

Organizations must implement reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, modification, and destruction, and should expeditiously notify individuals of security breaches that create significant risk of harm. Baseline precautions should apply to any collection of personal information, and additional measures should account for and be proportionate to the risk of harm.

Scope and Accountability

Hold organizations accountable for compliance.

Accountability can and should come in many forms. Lawmakers and regulators should set baseline requirements and enable flexibility in how to meet those requirements. Industry accountability programs and safe harbors can incentivize best practices, particularly in providing more flexible approaches to dealing with evolving technologies.

Focus on risk of harm to individuals and communities.

Regulators should encourage the design of products to avoid harm to individuals and communities. Enforcement and remedies should be proportional to the potential harms involved in the violation. Innovative uses of data shouldn't be presumptively unlawful just because they are unprecedented, but organizations must account for and mitigate potential harms. This includes taking particular care with sensitive information that can pose a significant risk. To enable organizations to develop effective mitigations, regulators should be clear about what constitutes a harm.

Distinguish direct consumer services from enterprise services.

Much processing of personal information is done by one company on behalf of another, where the processor lacks legal authority to make independent decisions about how to use the data or operate outside the bounds of the client's direction. Sometimes this distinction is described as "processors" versus "controllers", allowing for the efficient use of vetted, qualified vendors with minimal additional compliance costs, which is particularly important for smaller entities. Processors can look to the controller to meet certain obligations under the law, including transparency, control, and access, but processors must still meet basic programmatic and security responsibilities.

Define personal information flexibly to ensure the proper incentives and handling.

The scope of legislation should be broad enough to cover all information used to identify a specific user or personal device over time and data connected to those identifiers, while encouraging the use of less-identifying and less risky data where suitable. The law should clarify whether and how each provision should apply, including whether it applies to aggregated information, de-identified information, pseudonymous information or identified information.

Apply the rules to all organizations that process personal information.

Data is increasingly important through all sectors of the modern economy. Aside from the context of particular relationships that have existing rules, like with one's employer or attorney, legislation should apply to all economic sectors and all types of organizations that process personal information. While certain sectors (*e.g.,* healthcare) may have additional rules, regulation should set a baseline for all organizations. The application of the law should also take into account the resource con-

straints of different organizations, encouraging new entrants and diverse and innovative approaches to compliance.

Design regulations to improve the ecosystem and accommodate changes in technology and norms.

The technology involved in data processing is not static, and neither are the social norms about what is private and how data should be protected. A baseline law can provide clarity, while ongoing reviews (*e.g.,* rulemakings, codes of conduct, administrative hearings) can provide more flexible and detailed guidance that can be updated without wholesale restructuring of the legal framework. Governments can support these goals by rewarding research, best practices, and open-source frameworks. Creating incentives for organizations to advance the state of the art in privacy protection promotes responsible data collection and use.

Apply geographic scope that accords with international norms.

Data protection law should hew to established principles of territoriality, regulating businesses to the extent they are actively doing business within the jurisdiction. Extra-territorial application unnecessarily hampers the growth of new businesses and creates conflicts of law between jurisdictions. In particular, small businesses shouldn't have to worry about running afoul of foreign regulators merely because a few people from another country navigate to their website or use their service.

Encourage global interoperability.

Mechanisms allowing for cross-border data flows are critical to the modern economy. Organizations benefit from consistent compliance programs based on widely shared principles of data protection. Countries should adopt an integrated framework of privacy regulations, avoiding overlapping or inconsistent rules whenever possible. Regulators should avoid conflicting and unpredictable requirements, which lead to inefficiency and balkanization of services and create confusion in consumer expectations. In particular, geographic restrictions on data storage undermine security, service reliability, and business efficiency. Privacy regulation should support cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms that ensure protections follow the data, not national boundaries.

The CHAIRMAN. Thank you, Mr. Enright.

Mr. Kieran.

STATEMENT OF DAMIEN KIERAN, DATA PROTECTION OFFICER, TWITTER, INC.

Mr. KIERAN. Chairman Thune, Ranking Member Nelson, and members of the Committee, thank you for the opportunity to appear before the Committee today to discuss the important issue of consumer data privacy.

My name is Damien Kieran, and I am Twitter's Data Protection Officer. I lead Twitter's Data Protection Team responsible for the company's compliance with global data protection laws.

Twitter's commitment to privacy is why we are supportive of this committee's efforts to develop a robust privacy framework that balances the protection of individuals' rights and the preservation of the freedom to innovation.

We believe privacy is a fundamental right, not a privilege. That means when people trust us with their data, we should be transparent about and provide meaningful control over what data is being collected, how it is used, and when it is shared. We also believe the company should be held accountable to the people that trusts them with their data.

Privacy has been part of Twitter's DNA since it was created almost 13 years ago. When Twitter U.S. Company was founded, we offered a range of privacy ways for people to control their privacy,

from creating pseudonymous accounts to letting people control who sees their tweets and a wide array of granular privacy controls.

Those deliberate designs have allowed people around the world using Twitter to protect their privacy. It enables the free and open expression of opinions that Twitter is known for, including opinions that might otherwise be both personally and politically dangerous to share. It is part of Twitter's fabric.

That same philosophy guides how we protect the data that people share with Twitter. Twitter is public by default. This differentiates our service from other internet companies. In large part, it is what makes Twitter Twitter.

When an individual creates a Twitter account and begins tweeting, their tweets are public by default. Tweets are immediately viewable and accessible by anyone around the world, whether they have a Twitter account or not.

People understand the default public nature of Twitter and they come to Twitter expecting to see and join in public conversations. They alone control the content they share on Twitter, including how personal and private that content may be.

Twitter receives other information when people use our services. Our privacy policy has been designed to explain what data we collect, how it's used, and when it is shared.

Earlier this year, we undertook a ground-up revision of our privacy policy in an effort to make it easier to understand for our broad user base. We started with what people needed to know and built from there. It's a single document, not spread out over multiple web pages. It contains animations, graphics, and innovative pieces of technology in an effort to transparently explain what data we collect, how it is used, and when it is shared.

We plan to keep improving how we convey this information. We will always lead with transparency and openness.

We also provide the people that use our services, whether they have an account or not, tools that can allow them to have meaningful control over their data. For example, we provide individuals with the ability to limit the information collected and the ways in which it is used through controls, such as privacy and safety.

These data settings can be used to better personalize the individual's use of Twitter and allow him or her the opportunity to make informed choices about how Twitter collects certain data, the ways in which it is used, and how it is shared.

These settings are always easily accessible. Our most significant personalization data settings are on a single page. That page provides individuals with a single master switch that can disable all of these settings at once.

Twitter also makes available the Your Twitter Data Toolset. Your Twitter Data provides individuals insights into the type of data stored by Twitter, such as user name, e-mail address, and the phone number associated with the account, account creation details, and information about inferences we may have drawn. From this toolset, people can do things like edit their inferred interests and other information.

In addition, the Your Twitter Data Tool allows people with a Twitter account to download a copy of their relevant data from Twitter.

Since we updated the download tool on May 25, we've seen approximately 586,000 people around the world use the tool to download 560 terabytes of data.

In closing, Twitter already works to provide transparency and meaningful controls to the people that use our services. We believe the time is right for industry, civil society, and government to work together to develop a robust privacy framework that protects individuals' rights by ensuring transparency and accountability while preserving the freedom to innovation.

We stand ready to assist the Committee as it continues to explore options to ensure the privacy of Americans is protected.

Thank you and I look forward to your questions.

[The prepared statement of Mr. Kieran follows:]

PREPARED STATEMENT OF DAMIEN KIERAN, DATA PROTECTION OFFICER, TWITTER, INC.

Chairman Thune, Ranking Member Nelson, and Members of the Committee:

Thank you for the opportunity to appear before the Committee today to discuss the important issue of consumer data privacy.

Twitter's purpose is to serve the public conversation. We serve our global audience by focusing on the people who use our service, and we put them first in every step we take. People around the world use Twitter as a "town square" to publicly, openly, and freely exchange ideas. We must be a trusted and healthy place in order for this exchange of ideas and information to continue.

To ensure such trust, the privacy of the people who use our service is of paramount importance to Twitter. We believe privacy is a fundamental right, not a privilege. Privacy is part of Twitter's DNA. Since Twitter's creation over a decade ago, we have offered a range of ways for people to control their experience on Twitter, from creating pseudonymous accounts to letting people control who sees their Tweets, in addition to a wide array of granular privacy controls. This deliberate design has allowed people around the world using Twitter to protect their privacy.

That same philosophy guides how we work to protect the data people share with Twitter.

Twitter empowers the people who use our services to make informed decisions about the data they share with us. We believe individuals should know, and have meaningful control over, what data is being collected about them, how it is used, and when it is shared. And we believe that the time is right for industry, civil society, and government to work together to develop a robust privacy framework that protects individuals' rights by ensuring transparency and accountability while preserving the freedom to innovate.

This testimony provides information about the Twitter service, including (1) how people can communicate on Twitter; (2) the information we receive; and (3) an overview of how Twitter uses data and the tools Twitter provides individuals to manage their data.

I. Communicating on Twitter

Twitter was conceived and designed to be a platform for public conversation. This is the key feature of the service and what sets Twitter apart from many other Internet companies. When an individual creates a Twitter account and begins Tweeting, his or her Tweets are public.

Tweets are immediately viewable and searchable by anyone around the world, regardless of whether they possess a Twitter account. Similarly, when an individual follows another Twitter account or likes another Tweet, others can see the followed accounts and the Tweets that the individual liked. People understand the default public nature of Twitter and come to Twitter expecting to see and join in public conversations on topics that interest them. Thus, when individuals Tweet, they control the content they share, including how personal or private the content may be. This is how Twitter is designed and is a main part of the attraction and value proposition the platform provides to its customers.

While most people come to Twitter to join the public conversation, Twitter also provides a number ways to communicate non-publicly. For example, an individual can protect their account by changing their settings. If an individual protects his or her account, their Tweets will not be public by default. Instead, Tweets from pro-

tected accounts are only visible to the followers an individual has approved and will not appear in third-party search engines, like Google Search. Additionally, people can communicate with one another without Tweeting publicly by using the Direct Messaging feature.

II. Information Twitter Receives

Although the information people share on Twitter is generally public, Twitter also receives non-public personal information. For example, a person creating a Twitter account must provide the platform with his or her e-mail address or phone number. Twitter will also receive standard log information, such as the device being used and the Internet Protocol (IP) address. People who use the service may also choose to share additional information with Twitter including, for example, their address book contacts in order to connect with people they know, help others find and connect with them, and better recommend content to them and others.

In addition, and consistent with nearly all other online platforms, Twitter uses cookies and other similar technologies, such as pixels or local storage, to operate its services and help provide individuals on the platform with a better, faster, and safer experience. Cookies are small files that websites place on a computer as an individual browses the web. Like many websites, Twitter uses cookies to discover how people are using the services and to make them work better. Twitter also uses cookies to help serve people more relevant content based on where they have seen Twitter content on the web, and to serve targeted advertising. Twitter provides individuals with additional control over whether their data is used for these purposes.

In order to show people the most interesting and relevant content, Twitter may infer information about individuals based on their activity on the platform and other information. This includes inferences such as what topics people may be interested in, how old a person is, what languages a person speaks, and whether the content of one account may be of interest to others on the platform. For example, Twitter may infer that an individual is a basketball fan based on accounts the individual follows and suggest content related to the National Basketball Association. Inferences assist Twitter in offering better services and personalizing the content Twitter shows, including advertisements.

Twitter uses the data it receives to deliver, measure, and improve services in a variety of ways, including: protecting the services; authentication and security; remembering preferences; improving analytics and research, including Twitter Ads and Twitter buttons and widgets; customizing Twitter services with more relevant content like tailored trends, stories, advertisements, and suggestions for people to follow; and assisting in delivering advertisements, measuring their performance, and making them more relevant.

III. Transparency and Controls

Twitter believes individuals should know, and have meaningful control over, what data is being collected about them, how it is used, and when it is shared. Twitter is always working to improve transparency into what data is collected and how it is used. Twitter designs its services so that individuals can control the personal data that is shared through our services. People that use our services have tools to help them control their data. For example, if an individual has registered an account, through their account settings they can access, correct, delete or modify the personal data associated with their account.

A. Data Transparency

Twitter recently updated our Privacy Policy to include callouts, graphics, and animations designed to enable people to better understand the data we receive, how it is used, and when it is shared.

Twitter also provides a toolset called Your Twitter Data. Your Twitter Data tools provide individuals accessible insights into the type of data stored by Twitter, such as username, e-mail address, and phone numbers associated with the account and account creation details. The birthdays and locations of individuals are also shown in the tool if they have previously been provided to Twitter.

Individuals using the Your Twitter Data tool can also see and modify certain information that Twitter has inferred about the account and device such as gender, age range, languages, and interests. People on Twitter can review inference information, advertisers who have included them in tailored audiences, and demographic and interest data from external advertising partners. The Your Twitter Data tool also allows people with a Twitter account to download a copy of their relevant data from Twitter. We recently updated the download feature of the Your Twitter Data tool to include additional information. Since that update on May 25, 2018, we have seen approximately 586,000 people around the world use the tool to download 560 terabytes of data.

There is a version of this tool available to individuals who do not have a Twitter account, or for those logged out of the account.

B. Tools for Managing Data

When individuals on Twitter log into their accounts, they have immediate access to a range of tools and account settings to access, correct, limit, delete or modify the personal data provided to Twitter and associated with the account, including public or private settings, marketing preferences, and applications that can access their accounts. These data settings can be used to better personalize the individual's use of Twitter and allow him or her the opportunity to make informed choices about whether Twitter collects certain data, how it is used, and how it is shared.

For example, individuals can change the personalization and data settings for their Twitter account, including:

- Whether interest-based advertisements are shown to an individual on and off the Twitter platform;
- How Twitter personalizes an individual's experience across devices;
- Whether Twitter collects and uses an individual's precise location;
- Whether Twitter personalizes their experience based on places they have been; and
- Whether Twitter keeps track of the websites where an individual sees Twitter content.

An individual on Twitter can disable all personalization and data setting features with a single master setting prominently located at the top of the screen.

People on the platform can also deactivate their accounts. Deactivated Twitter accounts, including the display name, username, Tweets, and public profile information, are no longer viewable on Twitter.com, Twitter for iOS, and Twitter for Android.

C. Third Party Access to Twitter Data

To share the public content on Twitter as widely as possible, we provide companies, developers, and other customers with programmatic access to public Twitter data through Application Programming Interfaces, or APIs. Twitter only discloses private information of individuals at the persons' direction or if the settings of the individual allow personal data to be disclosed, to protect the safety of any person, to protect the safety or integrity of our platform, and to address fraud, security, or technical issues. We also disclose data as reasonably necessary to comply with valid legal requests.

1. Developers and Partners

The Twitter API provides broad access to public Twitter data that individuals have chosen to share with the world. Twitter also supports APIs that allow individual on the platform to manage their own non-public Twitter information (*e.g.,* Direct Messages) and provide this information to developers whom they have authorized.

New Enterprise and Premium API customers and data partners undergo a review process before they are granted access to Twitter data. That review examines the company's history, the proposed use of the data, and privacy and security considerations designed to prevent misuse of the data. Twitter routinely rejects use cases that do not comply with our rules, and we often require customers to revise and resubmit applications in order to ensure that they are in compliance with our policies.

In addition, our Developer Policy places a number of restrictions on how all developers—Enterprise partners as well as customers of our Premium and public APIs—may use Twitter data. Where warranted, Twitter takes enforcement action against applications found to be in violation of the Developer Agreement and Policy or the Twitter Rules.

2. Law Enforcement

In the limited circumstances in which the disclosure of private personal data to law enforcement is necessary, Twitter does so only in response to appropriate legal process such as a subpoena, court order, or other valid legal process—or in response to a valid emergency request.

To close, we believe privacy is a fundamental right, not a privilege. Twitter wants to empower all individuals who use our services to make the best decisions about the information they share with us. This is vital as the digital world we inhabit continues to evolve, change and impact our lives in important ways. The time is right for industry, civil society, and government to work together to develop a robust pri-

vacy framework that protects individuals' rights by ensuring transparency and accountability while preserving the freedom to innovate. We stand ready to assist the Committee as it continues to explore options to ensure the privacy of Americans is protected.

The CHAIRMAN. Thank you, Mr. Kieran.
Mr. Tribble.

STATEMENT OF GUY "BUD" TRIBBLE, VICE PRESIDENT, SOFTWARE TECHNOLOGY, APPLE, INC.

Mr. TRIBBLE. Good morning, Chairman Thune, Ranking Member Nelson, and members of the Committee.

I'm honored to be with you for this important hearing and to convey Apple's support for comprehensive Federal privacy legislation that reflects Apple's long-held view that privacy is a fundamental human right.

My name is Bud Tribble. I'm a physician. My research background includes neurophysiology and mechanisms of epilepsy. I'm also Vice President of Software Technology at Apple, where I began my career in 1981 working as Manager for the original Mac Software Team.

It was an exciting time to be at Apple back then. Computing was something that was done by third parties using big mainframes, until the debut of personal computers, like the Macintosh. Few people could have imagined the day when they would have a computer in their pockets and even fewer people could have imagined the amount of personal information that would be flowing in cyberspace.

To Apple, privacy means much more than having the right to not share your personal information. Privacy is about putting the user in control when it comes to that information. That means that users can decide whether to share personal information and with whom. It means that they understand how that information will be used.

Ultimately, privacy is about living in a world where you can trust that your decisions about how your personal information is shared and used are being respected.

We believe that privacy is a fundamental human right, which should be supported by both social norms and the law. This approach comes very naturally to Apple. We got our start by ushering in the personal computer revolution, putting the user in the driver's seat of their own computer.

When the Internet began greasing the skids on information flow, it seemed very natural and very important to extend that by putting users in control of their personal information.

Apple's about harnessing technology to empower people. We have proved time and again that great experiences don't have to come at the expense of privacy and security. At Apple, this has a fundamental effect on how we develop all of our products. Someone called this privacy by design. It means that we challenge ourselves to minimize the amount of personal information we collect.

Can the information that we do collect be less identifiable? Can we process information on the device instead of sending it to our servers? We want your device to know everything about you but we don't think that we should.

When we do collect personal information, we are specific and transparent about how it will be used. We do not combine it into a single large customer profile across all of our services. We strive to give the user meaningful choice and control over what information is collected and used, and we spend a lot of time designing the best way to present those choices and explain them to the user.

And, finally, we provide strong easy-to-use security to help ensure that privacy expectations are not destroyed by bad actors.

These concepts have guided our design process for years because privacy is a core value at Apple, not an obligation or an after-market add-on, and these are a few of the concepts that we believe this committee should consider as it undertakes the important task of drafting comprehensive privacy legislation that protects consumers and encourages continued innovation.

Mr. Chairman, members of the Committee, thank you for the opportunity to participate in this important hearing.

[The prepared statement of Mr. Tribble follows:]

PREPARED STATEMENT OF GUY "BUD" TRIBBLE, VICE PRESIDENT, SOFTWARE TECHNOLOGY, APPLE, INC.

Good morning Chairman Thune, Ranking Member Nelson, and members of the Committee. I am honored to be with you for this important hearing and to convey Apple's support for comprehensive Federal privacy legislation that reflects Apple's long-held view that privacy is a fundamental human right.

My name is Bud Tribble. I am a physician; my research background includes neurophysiology and mechanisms of epilepsy. I am also Vice President of Software Technology for Apple, where I began my career in 1981, working as manager for the original Macintosh Software team. It was an exciting time to be at Apple. Back then, computing was something that was done by third-parties using big mainframe computers until the debut of personal computers like Macintosh. Few people could have imagined a day when they would have a computer in their pockets. And even fewer people could have imagined the amount of personal information that would be flowing in cyberspace.

To Apple, privacy means much more than having the right to not share your personal information. Privacy is about putting the user in control when it comes to that information. That means that users can decide whether to share personal information and with whom. It means that they understand how that information will be used. Ultimately, privacy is about living in a world where you can trust that your decisions about how your personal information is shared and used are being respected. We believe that privacy is a fundamental human right, which should be supported by both social norms and the law.

This approach comes very naturally to Apple. We got our start by ushering in the personal computer revolution—putting the user in the driver's seat of their own computer. When the Internet began greasing the skids on information flow, it seemed very natural and very important to extend that by putting users in control of their personal information. Apple is about harnessing technology to empower people. We have proved time and again that great experiences don't have to come at the expense of privacy and security.

At Apple, this has a fundamental effect on how we develop all of our products. Some would call this "privacy by design." It means that we challenge ourselves to minimize the amount of personal information we collect. Can the information we do collect be less identifiable? Can we process information on the device instead of sending it to servers? We want your device to know everything about you; we don't feel that we should.

When we do collect personal information, we are specific and transparent about how it will be used. We do not combine it into a single large customer profile across all of our services. We strive to give the user meaningful choice and control over what information is collected and used. We spend a lot of time designing the best way to present those choices and explain them to the user. And finally, we provide strong, easy to use security to help ensure that privacy expectations are not destroyed by bad actors.

These concepts have guided our design process for years because privacy is a core value at Apple, not an obligation or an aftermarket add-on. And these are a few of the concepts that we believe this Committee should consider as it undertakes the important task of drafting comprehensive privacy legislation that protects consumers and encourages continued innovation.

Mr. Chairman, Members of the Committee, thank you for the opportunity to participate in this important hearing.

The CHAIRMAN. Thank you, Mr. Tribble.

Ms. Welch.

STATEMENT OF RACHEL WELCH,
SENIOR VICE PRESIDENT, POLICY AND EXTERNAL AFFAIRS,
CHARTER COMMUNICATIONS, INC.

Ms. WELCH. Good morning, Chairman Thune, Ranking Member Nelson, and members of the Committee. I'm pleased to have the opportunity to be here before you today.

My name is Rachel Welch, and I'm Senior Vice President of Policy and External Affairs at Charter Communications.

Charter values and relies on the trust and loyalty of our customers. We have more than 26 million across 41 states. Our network provides high-speed broadband, video, voice services to communities of all types and sizes.

One of our key business objectives is to provide our customers with a superior broadband experience that they value and will use.

Charter appreciates the Committee holding this important hearing to focus on the complex issue of online privacy. We also appreciate the developing dialogue among stakeholders, including those seated next to me here today, as well as by consumer groups, think tanks, and others who are also examining potential approaches to strengthen the privacy and security of consumers' online personal information.

Rapid changes in technology are making it difficult for consumers to protect their online data. Businesses now collect, analyze, and share consumers' personal online information in unprecedented volumes. While there are legal protections for certain categories of sensitive information, such as financial information or health data, vast amounts of other personal data are being collected, shared, tracked, and even sold online without any specific protection.

It is increasingly apparent that consumers need to know that their personal information is protected in order for them to continue to feel confident using online services.

That is why Charter has called for uniform Federal privacy protections that would require meaningful consent for all Americans, no matter where they go on the Internet. Charter believes that such a framework should focus on the following five principles.

The first is consumer control. Consumers should be empowered to have a meaningful choice for each use of their data. We believe the best way to ensure consumers have control over their personal information is to require online companies to obtain opt-in consent. This means that companies would be required to obtain an affirmative consent for any use of personal data other than to provide the service requested. This means no more pre-tick boxes, no take-it-or-leave-it offers, and no default consents.

The second principle is transparency. Consumers should be given the information they need to make an informed decision. Explanations about how companies collect, use, and maintain consumers' data should be easy to understand and readily available.

The third is parity. Consumers are best served by a uniform framework that is applied consistently across the entire online ecosystem. It should not be based on who is collecting the information or whether a service is free or paid.

The fourth principle is uniformity. For these protections to be effective, there should be a single national standard that protects consumers' online privacy. Whether a consumer's information is adequately protected should not depend on where they live or where they travel.

The final principle is security. At Charter, we believe privacy is security and security is privacy. Strong data security practices should include safeguards that protect against all unauthorized access to personal online information.

We support the adoption of Federal legislation that is based on these principles and we believe the FTC is the right agency to oversee and enforce any new privacy law.

Recent revelations about the vulnerability and misuse of online data have led to a long overdue discussion about what happens to our personal information online and how best to protect it.

We look forward to working with the members of the Committee and other stakeholders to develop legislation that protects consumers and makes them feel confident that they can take advantage of all the products and services that the Internet has to offer.

I thank the Committee for their time and I'm happy to answer any of your questions.

[The prepared statement of Ms. Welch follows:]

PREPARED STATEMENT OF RACHEL WELCH, SENIOR VICE PRESIDENT, POLICY AND EXTERNAL AFFAIRS, CHARTER COMMUNICATIONS

Introduction

Good morning, Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee. Thank you for the opportunity to appear today.

I am Rachel Welch, Senior Vice President, Policy and External Affairs at Charter Communications. I lead the team that develops our public policy positions here in Washington and across the 41 states we serve.

As a leading provider of broadband Internet services, Charter values and relies on the trust and loyalty of its more than 26 million residential and business customers. Our network provides competitively priced high-speed broadband, video and voice services to neighborhoods of all types, from large cities to small towns and rural areas, from Fortune 100 customers to small businesses across the country.

Fundamentally, one of our key business objectives is to provide our customers with a superior broadband experience that they value and use. To that end, we have invested more than $27 billion in broadband infrastructure and technology since 2014. The company has boosted starting speeds to 200 Mbps in roughly 40 percent of the markets we serve and 100 Mbps nearly everywhere else, with no data caps, no modem fees, no annual contracts and no early termination fees. We are also rolling out Spectrum Internet Gig which delivers a one gigabit connection to homes and businesses and we are on track to offer this service across virtually our entire footprint by the end of the year.

Charter appreciates the Committee holding this hearing and focusing on the complex issues that impact consumers' online privacy. We also appreciate the developing dialogue among stakeholders—including those seated next to me here today—as well as consumer groups, think tanks and others who have begun to examine potential approaches to protecting the privacy and security of consumers' personal information online.

Consumers Need a Comprehensive Online Privacy Framework

Advances in technology have radically changed the privacy landscape. Despite Americans' daily reliance on websites, apps, and social media, it is difficult for consumers to understand and appreciate how companies are collecting, analyzing, sharing and selling a tremendous amount of information about them.

An increasingly important aspect of ensuring that consumers continue to utilize all the services the Internet has to offer is making sure that they are confident that their personal information online is protected. While we strive to give our customers confidence with our current policies and practices such as not selling any information that personally identifies our customers to third parties, we recognize that there is still more to do.

That is why, last April, Charter CEO Tom Rutledge called for uniform privacy protections that would provide more meaningful consent for the use of their online information for all Americans no matter where they go on the internet. We believe that a uniform national framework establishing strong online privacy protections and data security is needed to give all consumers, including our customers, confidence that their privacy is protected. We believe that this framework should seek to empower and inform consumers through rules that address five core principles—control, transparency, uniformity, parity and security.

Businesses now collect, analyze, and share consumers' personal online information in unprecedented volumes. While there are legal protections for certain categories of particularly sensitive information, such as financial information and health-related data, vast amounts of other personal data are being collected, shared, tracked, and even sold online without specific protections.

Threats to privacy and security are pervasive on the Internet today. Consumers' personal data is exposed to more entities than ever before and much of this data collection happens without their knowledge. For example, most websites embed tracking and advertising links throughout their pages. The consumer's web browser is directed by the destination site to make requests to many unrelated sites instead of requesting content only from the intended destination. These sites collect user information and insert cookies into their browser. This enables third parties to track where the user goes online and stitch together their online behavior to build a comprehensive, highly individualized profile about him or her.

Rapid changes in technology have also made it more difficult for consumers to protect their online data. While some consumers can take steps to try to prevent certain collection activities that may be more well-known—such as by disabling cookies on their web browsers or disabling location services—they may not be aware of other practices that are not visible when they surf the web or fire up the latest new device or app. For instance, third-party ad networks and online data brokers are often invisible to consumers. Moreover, technology and data collection practices are constantly evolving, which can further impede consumers' efforts to protect themselves.

Online Privacy is A Critical Part of Ensuring Economic Security

The Internet has been a vibrant engine of economic growth and innovation for the last 20 years. Consumers in the United States and around the world rely more and more on the Internet to conduct their daily lives. Websites and apps are used to find jobs, shop for groceries, take classes, manage finances, connect with loved ones, plan travel, find dates, and be entertained. Exciting new applications and use cases, such as telehealth and telemedicine, offer tremendous potential to bring similar disruption to other sectors of the U.S. economy and create thousands of new American jobs. For the Internet to continue to deliver on this promise, however, users must continue to feel confident in their ability to control their online data.

Unfortunately, according to data collected for the National Telecommunications and Information Administration (NTIA) by the U.S. Census Bureau, nearly half of Internet users in the United States refrained from online activities due to privacy and security concerns. Similarly, a recent survey by Parks Associates showed that approximately 45 percent of consumers are "very concerned about people accessing their devices or data without permission" and consider data privacy and security issues to be "their greatest concern about connecting devices to the internet."

A comprehensive legal framework for online privacy that empowers and informs consumers will increase consumer confidence in online services. If the framework is competitively neutral and reflects the principle of parity, it would not impede businesses from developing new technologies or business models that will encourage market entry, innovation, and robust competition. Instead, it would ensure that businesses have the necessary incentives to develop new products and services that both benefit consumers and earn their trust.

It's on all of us to develop a comprehensive framework that will help Americans avoid uncertainty and enable continued innovation economic growth in the future. We believe that a Federal framework is the best path forward.

Five Principles for Protecting Consumers Online

We appreciate that Congress is taking up the issue of online privacy and data security and recognize that there are a range of ideas and methods for protecting online data. We believe that a national online privacy framework should start with the consumer and be grounded in the concept of empowering and informing consumers to control the personal information that is collected about them online.

Charter believes such a framework should focus on the following core principles.

The first principle is *control.* Consumers should be empowered to have meaningful choice for each use of their data. We believe the best way to ensure consumers have control over their data is through opt-in consent. Any legal framework that is ultimately adopted should ensure consumer consent is purposeful, clear and meaningful. That means no more pre-ticked "boxes," take-it-or-leave-it offers, or other default consents. It also means that the use of personal data should be reasonably limited to what the consumer understood at the time consent was provided. Companies also should ensure that consent is renewed with reasonable frequency.

The second principle is *transparency.* Consumers should be given the information they need to make an informed decision. Explanations about how companies collect, use and maintain consumers' data should be clear, concise, easy-to-understand and readily available. Privacy policies should be separate from other terms and conditions of service. If all online entities provide such transparency, consumers will have the ability to weigh the potential benefits and harms of the collection and use of their personal data, and truly provide informed consent.

The third principle is *parity.* Consumers are best served by a uniform framework that is applied consistently across the entire Internet ecosystem not based on who is collecting it, or whether a service is free or paid. From a consumer standpoint, they want their online data protected whether they are using an ISP like Charter, a search engine, an e-commerce site, a streaming service, a social network, or a mobile carrier or device. Quite simply, we believe consumers should know that their personal information is being treated with the same level of protections wherever they go on the Internet.

The fourth principle is *uniformity.* For these protections to be effective there should be a single national standard that protects consumers' online privacy regardless of where they live, work or travel. Whether a consumer's information is adequately protected should not differ based on which state he or she is logging in from. A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation on the internet—which is a borderless technology.

The final principle is *security.* At Charter we believe privacy is security and security is privacy. Strong data security practices should include administrative, technical, and physical safeguards to protect against unauthorized access to personal data, and ensure that these safeguards keep pace with technological development.

We support the adoption of legislation that is based on these principles. We also believe that the Federal Trade Commission is the appropriate agency to oversee and enforce online privacy and data security. The FTC is the Nation's leading agency when it comes to privacy enforcement, having brought hundreds of privacy and data security cases. Importantly, it has broad authority to safeguard consumers and enforce privacy protections across the entire online ecosystem. As a result we believe that the FTC is the right agency to oversee and implement any legislative framework.

Conclusion

Revelations of data misuse in recent years have led to a long-overdue public conversation about what happens to data online and the vulnerabilities that develop when online data goes unprotected. Consumers today and in the future deserve to have the ability to control how their information is collected and used whenever they use the internet, and wherever they go online.

As our CEO Tom Rutledge has said, different policies that lead to inconsistent protections sow confusion and erode consumers' confidence in their interactions online; this is bad for business and bad for America since it threatens the Internet's future as an engine of economic growth.

Charter looks forward to the opportunity to work with Members of Congress, industry partners, consumer groups and other stakeholders to develop legislation that protects consumers, and makes them feel more confident taking advantage of all that the Internet has to offer.

I thank the Members of the Committee for the opportunity to appear before you today on this important issue, and I would be happy to answer any questions you might have.

The CHAIRMAN. Thank you, Ms. Welch.

There are a number of you who represent companies today who are operating in Europe and so you've had several months now working under the GDPR and all of you have undoubtedly begun to consider what it would mean to comply with California's new law, the CCPA.

So I have three related questions about these laws, and the first is if we pursue Federal legislation in this space, can you identify one or more provisions from either law that we should emulate? Anybody? Mr. Cali?

Mr. CALI. Yes, both the laws apply to all companies uniformly, and I think that's a very positive element of both laws that should be emulated.

In addition, I would note that California sets the default as opt-out and while you may not adopt that particular framework, what it does underscore is there is value in the use of data and it's recognized by that default setting.

The CHAIRMAN. Nobody else? Then if there are conflicts between the two—are there conflicts, I should say, between the two, between California and GDPR, that we should address in a Federal law? Mr. Cali?

Mr. CALI. Thank you. I think the concerns on both are slightly different but significant. So GDPR, the difficulty and challenges, it's overly prescriptive and extremely burdensome, and while the results are early, you see websites have gone dark, hundreds of websites have gone dark. More companies have exited Europe or appear to exit Europe, startup companies, and it looks like it's actually strengthening the large incumbent platforms in Europe, and on top of that, it may, because of the limits on datasets, hurt innovation, things like lot chain and artificial intelligence.

California has a number of concerns raised. One, and probably the most significant, is it's a single state and if other states follow suit, we'll be facing a patchwork of rules and fragmentation that will be just unworkable both for consumers as well as mobile companies and internet companies.

And then we do have concerns. California has a non-discrimination obligation that sounds good in statement. It's ambiguous. It may deny consumers the ability to receive benefits from consumers for sharing their data and this could affect things as commonplace as your grocery loyalty card program where you get a benefit for sharing information with your grocery store on your purchases.

We're also worried about the notice and consent process because it tends to be serial. It's complex, and it may end up restricting data far more than anyone else anticipated.

So what we're urging is a comprehensive Federal law that looks at both of these laws, learns from them, but does better than them.

The CHAIRMAN. Does your company or any of your companies plan to seek any revisions to the California law before it takes effect?

Mr. CALI. Yes, AT&T will seek revisions to the law. We are concerned about the non-discrimination obligation, as I say, notice and consent.

We're also looking at implementation periods. They're very tight. There are some other things very particular to the law that we are going to work with the legislature and the state AG, who's doing the rulemaking on it.

The CHAIRMAN. So you mentioned in one of your answers there the issue of GDPR's specific requirements for handling retention and deletion of data. You mention it in your answer but that's something that I understand is an issue.

So do you think that those types of requirements are going to make it harder for companies to launch and prevent barriers to entry? You mention in your response that you're already seeing the incumbents benefiting from this, but is it going to be harder to get startups launching and at least cause them to avoid doing business in the EU?

Mr. CALI. I think there are a host of burdens associated with the GDPR that perhaps if it existed at the time the companies at this table started, we wouldn't be here. None of them would be here.

In terms of the rights to access, deletion, portability, we support the concepts, but we need to be mindful there are cyber security concerns. There are fraud and authentication concerns. There are cost concerns in terms of deploying the systems and the time that will need to be taken to do that.

And on portability in particular, we have to make a judgment about whether it will enhance competition and help smaller companies or actually embed the incumbents where they are. So I think those are a number of questions raised by the GDPR that need to be addressed.

The CHAIRMAN. Anybody else want to talk about compliance costs under GDPR today and whether you think those raise barriers that prevent barriers to entry for startups?

Mr. ENRIGHT. Senator, on the Google side, we certainly recognize the compliance obligations under the GDPR have been a tremendous challenge for us. We took them very seriously. We are confident in our compliance posture, but we encourage the Committee in contemplating future legislation when you are looking at the GDPR as a reference point to carefully consider this point because organizations like Google are clearly better positioned to absorb the kinds of compliance costs that a rigorous regulatory regime like that required under the GDPR could create for small-and medium-sized businesses.

Ms. WELCH. Mr. Chairman, if I might add, we're a domestic-based ISP and so our services are focused here in the U.S. So we are not subject to GDPR. So we're watching it and recognize that it's a model that folks are looking at, but we don't know what it will take for us to implement it, what the costs will be, what new systems we may have to build. There will be a number of other companies across the U.S. that will have those same concerns.

So as you're looking at the GDPR, I think it's important for this Committee, and we're glad that you're having this hearing today to start the conversation, to put its own stamp on what the U.S.

framework should be for privacy protections to ensure that companies can comply, that we have enough time to comply.

So we certainly see that common principles marching in terms of control, transparency, and equal treatment of data across the sector, but I would just say that there are certain things that we just don't even know what it will mean to implement here in the U.S.

The CHAIRMAN. Thanks. Mr. Tribble?

Mr. TRIBBLE. Yes. You know, I think with the exception of here, most of the other companies at this table have gone through the process and are probably of the size well able to take on the implementation work necessary to implement the GDPR.

I'd like to point out, you know, we have an app store with six million developers in the U.S. Many of those are small-and medium-size businesses and so I think it's very important in looking at legislation to look at those small and medium businesses and what the burden will be on them as far as recordskeeping and so forth. I think it would be very important to make sure that it's not over-burdensome for that class of companies.

Probably the companies at this table have enough resources to deal with it, but we're concerned about that small-and medium-size business.

The CHAIRMAN. Thank you.

Senator Nelson.

Senator NELSON. The FTC is primarily responsible for protecting consumer privacy in the commercial marketplace. Yet it has a relatively small staff with limited resources.

Could each of you tell me and the Committee, will your companies support Congress providing the FTC with more resources and personnel to more effectively do its job to protect consumer privacy?

Mr. CALI. Yes, Senator, we would. In a properly structured bill, that would be an appropriate step.

Mr. DEVORE. Yes, Senator, thank you. On behalf of Amazon, we would. Enforcement is a critical piece of the puzzle and the FTC should have the resources it needs to investigate and enforce rigorously.

Mr. ENRIGHT. Yes, Senator. From Google's perspective, notwithstanding the resource constraints you describe, our experience with the FTC is that they have been a rigorous and effective enforcement agency in the context of privacy and we would support, as others have said, a reasonable allocation of resources to further their work.

Mr. KIERAN. Yes, Senator. Much like my colleague, Mr. Enright, Twitter has enjoyed a very good relationship with the FTC and hopes that that continues, and we'd welcome the opportunity to understand how we could best help them going forward.

Mr. TRIBBLE. Yes, Senator. Apple agrees that FTC should get the resources they need as a part of comprehensive legislation.

Ms. WELCH. Senator, Charter agrees, as well. If they need more tools, we should work with you to get them for them.

Senator NELSON. Well, under current law, the FTC can only bring an enforcement action against a company that violates the terms of its own public policy or its own public privacy policy, and they can only do so under their organic authority of the FTC Act.

It prohibits, and the statute reads, "Unfair or deceptive acts or practices." Basically, the FTC can bring an enforcement action if a company lies.

Do you support providing the FTC with more legal authority and better tools to protect consumer privacy?

Mr. CALI. Senator, I'd start by saying we don't support unfettered discretion in any agency. We believe it's Congress's job to give direction, set policy, and set up the guardrails.

But if Congress were to do that, as I indicated earlier, we would support working with the Committee in finding the proper tools for the FTC to do its job and do its job effectively.

Mr. DEVORE. Thank you, Senator. I think the starting point for us, as with all of these issues, is to think about what benefits customers and the core principles of assuring that customers understand how their data is being used, that they get the benefit of products and services that use their data carefully and sensibly in line with their expectations.

As you said, the FTC does have authority now to get at violations of those kinds of principles and we welcome the opportunity to work with Congress to think through the clarification exercise that I understand this is the beginning stages of.

Senator NELSON. The question is not whether or not you want to work with Congress. The question is do you want to provide the FTC with more legal authority and better tools to protect consumer privacy?

Mr. DEVORE. Understood, Senator. I think the answer to the question is yes, but, of course, these issues are complex and the details matter a lot.

Mr. ENRIGHT. Senator, reviewing the FTC's track record of enforcement in the context of privacy and data protection over the last 20 years, I think there is a tremendous amount of evidence that as they have interpreted their unfairness and deception authority under the FTC Act, they've been a very effective and rigorous regulator in this space.

That said, like my colleagues, we would certainly be interested in engaging in a conversation about what an extension of their authority might look like and what the proper contours might be.

Senator NELSON. So is that a yes, maybe to——

Mr. ENRIGHT. That is——

Senator NELSON.—protect consumer privacy?

Mr. ENRIGHT. I would suggest that we first look at whether their existing authority is enabling them to exercise their mission effectively and if the answer to that question is no, then I think you move on to the question of expanding their authority.

Mr. KIERAN. Thank you, Senator. For Twitter, accountability is a key component of the way we work and so we view any Federal framework, whether that's empowering the FTC or otherwise, to make sure that it grapples with those questions of holding industry accountable.

We'd be supportive of engaging in more dialogue to understand how we could best work with the FTC or other mechanisms that might further that requirement of accountability.

Senator NELSON. So your answer is that you just want to work with the Committee. The question is more authority and legal tools to protect consumer privacy.

Mr. KIERAN. Senator, we do think that accountability is something that needs to be put in place to ensure the protection of consumers, and we think there are a variety of ways to get at that, and we just want to make sure that we're balancing appropriately those protections for individuals while also allowing the freedoms to innovate, whether that's with the FTC or otherwise.

Senator NELSON. So is that an I don't know?

Mr. KIERAN. No, Senator. It means we'd welcome the opportunity to understand more about how we would enable the FTC to do that, if the FTC is the chosen mechanism or path, but we think that there needs to be a fulsome discussion of how best to give teeth to accountability.

Senator NELSON. Seems to me that protecting consumer privacy ought to be an easy answer.

What about you, Mr. Tribble?

Mr. TRIBBLE. Well, I actually agree with Google that the FTC has a good track record here and I think it would be important to look at whether their existing legal authority is sufficient for them to enforce whatever comes out of this bill.

Enforcement, effective enforcement is important, but the mechanism that's used to do that ought to be fully informed by what's working now.

Senator NELSON. Ms. Welch?

Ms. WELCH. Senator Nelson, we believe that if the Committee finds that the FTC needs additional tools, they should have them, and we would like to work with you in order to accomplish that, and we believe that any Federal framework is obviously going to need enforcement tools and so we support that.

Senator NELSON. Thank you.

The CHAIRMAN. Thank you, Senator Nelson.

Senator Fischer.

STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Thank you, Mr. Chairman.

I'd like to follow the Ranking Member's line of questioning a little bit here and maybe dig down into it a little bit more.

We can't ignore the fact that we live in an economy that incentivizes the gathering of as much data as possible, to either use it or to sell it, and as Congress is looking to strengthen the privacy, I think it's crucial that we prevent irresponsible data use.

Mr. Tribble, do you think Federal legislation is needed to protect consumers from some of the aggressive data practices? You talk about, you know, more tools, but first you have to have legislation and if you feel it's needed, what would you suggest?

Mr. TRIBBLE. Yes, we believe that comprehensive Federal legislation is needed to help protect consumers, and, you know, the reason for that is that, as Chairman Thune pointed out, there's a history of increased personal information flowing on the Internet.

I have oodles of information about my life sitting in my pocket right now. That wasn't true five or 10 years ago. That is only going

to increase. So, yes, we think that the comprehensive Federal legislation is very important.

Senator FISCHER. And you brought up your concern about how that might burden smaller businesses.

So I guess what do you think would be the best approach to Federal legislation so we don't see that burden on smaller businesses where they have compliance issues, the costs associated with that?

Mr. TRIBBLE. Yes, I think anything that can be done to help make things clearer, make it so that businesses have one set of rules instead of many sets of rules to follow, and there may be other things.

For example, we worked with the Office of National Coordinator for Health IT to come up with a model privacy notice for apps that use health information and it's very helpful to us to be able to point our app developers, which we do, we link to the ONC site, and, you know, these smaller companies may not have teams of lawyers to draft things but that kind of thing can be very helpful, I think, to small and medium businesses.

Senator FISCHER. And when we look at consumers' personal data, it can be used in reasonable ways and unreasonable ways. What's an unreasonable way? What's an example of that?

Mr. TRIBBLE. Well, personal data can be used in ways that are, first of all, unexpected or not appreciated by the person whose data it is but specific ways, identity theft is an example of that. Simply information used out of context can be very misleading and affect someone's life. Information that is gathered on a person may be used to discriminate against them. So there are many ways that information can be used inappropriately and once it's collected, it's often very hard to keep track of it. So sometimes those things happen.

Senator FISCHER. Should companies focus on using data in ways that don't directly link to individual identity? For example, how can differential privacy advance efforts to reasonably minimize data collection, and can that be deployed at scale?

Mr. TRIBBLE. Well, at Apple, you know, we're always challenging ourselves to see if we can provide a great service or product without collecting as much information, and there are actually an increasing number of tools to do that.

One technique you mentioned is to disassociate the data from an identifier. I think it's important to realize that there's no silver bullet here because even information that has been disassociated from an explicit identifier, we've learned, can be later, you know, reassociated with that individual. Nonetheless, that action is helpful.

With respect to things like differential privacy, those are some newer technologies that allow us to collect information about a group of people without collecting any single individual's information.

For example, if I wanted to know the average amount of money a committee member had in their wallet, I could ask you, tell me how much money is in your wallet, but subtract or add a random number between, you know, a hundred dollars and then tell it to me. If I average those together, that's going to be—well, there are not enough committee members, but if there were thousands of you, it would be enough to tell me what your average amount of

money in your wallet is without me getting the information about any particular individual.

So those kinds of techniques, as well as using processing on the device or intelligence on the device to provide a service. For example, the iPhone will tell you where you parked your car. We don't have to send where you parked your car back up to Apple, your device can have enough intelligence to remember where you parked your car. So there are different ways you can implement the same service, some are more privacy-friendly.

Senator FISCHER. Thank you.

The CHAIRMAN. Thank you, Senator Fischer.

Senator Klobuchar.

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

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you for holding this important hearing. Thank you to all of you for appearing here today.

I think you all know this comes at a critical moment when we are, for the first time, seriously looking at privacy legislation.

Senator Kennedy and I have introduced the bipartisan Social Media Privacy, Protection, and Consumer Rights Act, and that is due to what we've seen with privacy violations for people in this country and the bill would make privacy disclosures more transparent, give consumers the right to control their own data by allowing people to opt out of having their data collected, and require companies to notify consumers of a privacy violation. In our legislation, the standards and enforcement are centralized at the FTC.

So I guess I'd start with one simple question. Do you all believe that we need some kind of Federal legislation to take place here so that we have some kind of privacy standard for consumers? Is there anyone that wants to—— Mr. Cali?

Mr. CALI. Yes, we have long supported a comprehensive Federal legislation and we do think it is important to protect consumers.

Senator KLOBUCHAR. OK. Anyone else? Mr. Enright?

Mr. ENRIGHT. Yes, we, too, at Google support broad Federal privacy legislation. We think it will benefit both consumers and the ecosystem of data-driven innovation.

Senator KLOBUCHAR. Mr. Kieran.

Mr. KIERAN. Like Google, we support Federal legislation.

Senator KLOBUCHAR. OK. Now when Mr. Zuckerberg was here, I asked him about this idea of the 70 TAR Notification after a breach. Is there anyone that favors that? He said that it could make sense. Anyone? No one favors that? OK. I'm going to take that as a no.

OK. Then the other piece of the legislation makes for simple language because so many of these privacy policies on your sites are very difficult to understand and our bill requires that online platforms make plain language disclosures regarding how personal data will be collected and used. Do you think that would make sense to do something like that? Anyone? Mr. Enright?

Mr. ENRIGHT. Yes, in connection with our privacy policy, we actually take a great deal of pride in the fact that a cross-functional team of attorneys, technologists, and user experience designers are

perpetually working on making our privacy disclosures as simple and accessible as possible and we have received praise publicly for the work in that area.

Senator KLOBUCHAR. OK. Mr. Kieran?

Mr. KIERAN. Like Google, we take pride in our privacy policy. In fact, this year we revised it completely. We started to consider how people would understand the basic information that they needed to have about the type of information we collect, when we use it, and when we share it, and what we actually did was we shared it with non-lawyers, non-policy people, and we asked them what issues they had in trying to understand it.

We then went back, reconsidered those concerns, and then we worked in clever things, like animations, graphics, pop-ups. We don't view that work as complete. We don't view it as static. The goal is to keep iterating on it and evolving to ensure that people do truly understand what we're doing with their data.

Senator KLOBUCHAR. So speaking of static, our bill would actually also include a provision that a consumer could withdraw consent to the terms of services just as easily as they're able to give consent. Do you think that would be helpful, Mr. Kieran, to include that?

Mr. KIERAN. Thank you, Senator. We already provide a variety of ways in which people who share information with us can opt out of sharing afterwards. We provide a set of tools from our privacy panel that allows people to determine what information they're sharing with us. So we do think it's an important component.

Senator KLOBUCHAR. OK. So do people have problems with an opting-out idea? No? OK. Good.

I think I'll just use my last minute here on the—and there are obviously remedies. I'll ask those questions in writing under the bill.

The Honest Ads Act, and I'll ask you about that, Mr. Enright. We've gotten support for that bill. It's a bill I have with Senator Warner and, sadly, Senator McCain's no longer with us, but he was the lead Republican on the bill, and you know what it does. It says that for online political ads, there has to be disclosure and disclaimers, including for issue ads.

Facebook and Twitter have both indicated that they support the bill, and Google has so far declined, and you are the biggest seller of online ads and expected to bring in roughly 40 billion in digital ad dollars in 2018.

So could you talk about where you are on the bill and what you think needs to be done?

Mr. ENRIGHT. Certainly, Senator. To be clear, my area is privacy. So the issue of political ads is not squarely within my domain.

That said, we appreciate your leadership on this issue. We do support the goals of your bill and we look forward to working with your staff to move it forward.

Senator KLOBUCHAR. OK. And I do think that this has something to do with privacy because a lot of these political ads that have come from Russia and other places have interfered with people's privacy.

Mr. ENRIGHT. Certainly. I agree with you, Senator.

Senator KLOBUCHAR. They've used photos of people that didn't consent to have them used. They falsified—the ads were obviously false and they brought people to rallies and did all kinds of things that were false and so I think you should think of it as not just sort of a thing over at the FEC, a political issue. It really goes to the fundamental misuse of the Internet.

Mr. ENRIGHT. I agree with you and I recognize that this is certainly relevant to the privacy conversation. It also, of course, involves other executives and teams at Google, but, again, to reiterate what I've said, we do support the goals of your bill and we're looking to working with your staff.

Senator KLOBUCHAR. Thank you.

The CHAIRMAN. Thank you, Senator Klobuchar.

Senator Moran.

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

Senator MORAN. Chairman Thune, thank you.

I chair the Subcommittee on Consumer Protection and Data Security of this Committee, and I'm certainly committed to ensuring that consumers' personal data is collected, used, transferred, and stored responsibly with appropriate transparency provided by you in the industry.

I do have concerns with the risks posed by the EU's General Data Protection Regulations and the California Consumer Privacy Act. Those concern what it will mean to the Internet ecosystem, especially the innovative entrepreneurial businesses that are positioned to be disadvantaged based upon these regulatory overhauls and in some instances these regulations conflict one with another.

In the interest of protecting Americans from data misuse and establishing certainty for businesses so that we can continue to create jobs and innovate and compete in this global economy, I've been working with Senator Schatz, with Senator Wicker, and with Senator Blumenthal to collect the thoughts of all interested parties, including consumer advocates, industry representatives, academics, academicians, and to identify responsible Federal privacy standards, and we most recently have sought for coordination with the Department of Commerce in a recent letter we sent to Secretary Ross last week.

I appreciate your willingness to testify today and I appreciate your perspectives.

I've heard from parties who are concerned that the recently adopted California Consumer Privacy Act, which takes effect in 2020, could influence other states to enact their own versions of those regulations. This could lead to a patchwork of state privacy laws that internet companies engaging in interstate commerce would need to navigate in order to remain compliant.

As some of you have mentioned, this is likely to have an unintended yet harmful impact on consumers due to confusion stemming from the uneven state-specific privacy requirements and choices.

Additionally, entrepreneurial businesses with less resources than the companies represented at the table today would be unfairly

precluded from engaging in the Internet due to the complexity of regulations and compliance costs.

A yes or no question for each of you. Would your company support Federal legislation to preempt inconsistent state privacy laws in the interest of providing clear privacy expectations for consumers and businesses?

Mr. CALI. Yes, Senator. In fact, Federal legislation will be of very little help if it just becomes the 51st layering on top of 50 state rules. We need a comprehensive but singular privacy framework and it should be a Federal preemptive framework.

Senator MORAN. Thank you. You answer yes or no questions like I do. Thank you.

[Laughter.]

Mr. DEVORE. Thank you, Senator. Yes, as I mentioned in my opening remarks, we do have concerns about the California law, in particular in the risk of a patchwork of uneven and disparate laws, I think won't serve the core interests in protecting customers' privacy.

Senator MORAN. Thank you.

Mr. ENRIGHT. Yes, Senator, and I would point the Committee back to our recently published Legislative Framework for Privacy and Data Protection as one instructive point in this conversation.

Senator MORAN. Thank you.

Mr. KIERAN. Yes, Senator, we would support that. What I would also say is that Twitter's experience is that we are actually quite a small company. We have only 3,300 approximately employees around the world. So we do tend to feel the burden of a disproportionate regulation.

So we think that it is important that there is a Federal framework put in place to prohibit a patchwork of state-by-state laws.

Senator MORAN. Thank you.

Mr. TRIBBLE. I think it would be helpful to prohibit a patchwork, but I think it's very important from the standpoint of the consumer that the bar be high enough on the Federal legislation to provide protection to the consumer that's effective.

Senator MORAN. Thank you.

Ms. WELCH. Senator, we agree, as well, and we believe that there needs to be a strong Federal framework, as well, and we think that consumers should be empowered with the ability to control their data through an opt-in.

Senator MORAN. Thank you. I support privacy rules that afford consumers the same protection no matter where they are in the Internet ecosystem.

Would you agree that regulating and enforcing privacy rules based upon the sensitivity of the data collected, used, transferred, and stored is the preferred approach and in the best interests of consumers in terms of certainty and transparency? Again, I think this can be a yes or no answer.

Mr. CALI. Yes.

Senator MORAN. Thank you.

Mr. DEVORE. Yes, Senator.

Senator MORAN. Thank you.

Mr. ENRIGHT. Yes, Senator.

Mr. KIERAN. Yes, Senator.

Mr. TRIBBLE. Yes.
Ms. WELCH. Yes.
Senator MORAN. As a follow up to that and the Senator from Florida, the Ranking Member, talked about the FTC, would you agree that the FTC is the appropriate Federal agency to enforce any future Federal privacy standards? Again, a yes or no.
Mr. CALI. Yes.
Mr. DEVORE. Yes, Senator.
Mr. ENRIGHT. Yes, Senator.
Mr. KIERAN. Yes.
Mr. TRIBBLE. I think they have a role. I think effective enforcement is important, but I think there may be options on additional enforcement mechanisms. So I guess that's a qualified yes.
Senator MORAN. Thank you.
Ms. WELCH. Yes.
Senator MORAN. Mr. Enright, I had a question for you in particular. I've run out of time, but I'll be back talking to you, I hope, if we have an additional round on data portability in your testimony.
Thank you very much.
The CHAIRMAN. Thank you, Senator Moran.
Senator Schatz.

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

Senator SCHATZ. Thank you, Mr. Chairman. Thank you all for being here.
We're here at least partly because a lot of you are worried very much about just GDPR and also the California law, so let's lay that out, and you want something that you can work with so you don't have to navigate 50 different statutory frameworks.
I understand that, and I think there's an opportunity to do something meaningful, but as Mr. Tribble said, we should make sure that we do something meaningful, and I understand that from the standpoint of some of these companies, the Holy Grail is preemption, and I want you to understand that you're only going to get there if this is meaningfully done. You're only going to get there—we're not going to get 60 votes for anything and replace a progressive California law, however flawed you may think it is, with a non-progressive Federal law.
So the first question I have, and it is a yes or no, is do you think companies ought to take reasonable steps to prevent unwanted disclosures of data and that companies should not use data to the detriment of their customers? Mr. Cali, and, please, yes or no.
Mr. CALI. Yes.
Mr. DEVORE. Yes, Senator, absolutely.
Mr. ENRIGHT. Yes, Senator, consistent with the principles we just published.
Mr. KIERAN. Yes, Senator.
Mr. TRIBBLE. Yes, Senator.
Ms. WELCH. Yes, Senator Schatz.
Senator SCHATZ. Thank you. I want to dig into the questions that Senator Nelson and others have asked about the FTC's authority.

I think it matters very much if we're going to write a new Federal privacy law that the FTC has rulemaking authority under APA, and I think it's a little bit of a sleight of hand. This may just be an opener, but some of these companies are saying we want new Federal law, we want to preempt the states from acting, but we don't really want to give the FTC the authority to make new rules in this space.

The kinds of laws that stand the test of time are the kinds of laws that articulate broad principles and that empower the expert agency to flesh that out over time and so do you support rulemaking authority in this new Federal privacy statute?

Mr. CALI. So, Senator, I agree with your earlier statement. We expect the comprehensive Federal law to be robust.

As I earlier mentioned, we are always worried about unfettered discretion in an agency.

Senator SCHATZ. I'll just remind you it's a yes or no.

Mr. CALI. Yes. So the point is——

Senator SCHATZ. I'll take that as a no.

Mr. CALI. No, no, it's not a no, and that's what I want you to know. We're not here digging lines in the sand.

Senator SCHATZ. I'll take that as a maybe.

Mr. CALI. A qualified yes.

Senator SCHATZ. I'll take it as a qualified even better than maybe.

Mr. CALI. Thank you.

Senator SCHATZ. Go ahead.

Mr. DEVORE. Thank you, Senator. For us, the answer is a qualified yes. The details matter tremendously. Innovation's critically important. Customer trust is critically important. We'd like to be able to achieve those things in any——

Senator SCHATZ. Fair enough. I'll start taking qualified yeses. Go ahead.

Mr. ENRIGHT. Also a qualified yes. I think this is one consideration that has important points of interplay with other aspects of a comprehensive bill.

Mr. KIERAN. Qualified yes, as well, Senator.

Senator SCHATZ. Come on, Apple. Just give me a yes.

Mr. TRIBBLE. Well, effective enforcement is critical but qualified yes as to the exact mechanism.

Ms. WELCH. Qualified yes, as well.

Senator SCHATZ. I just want to sort of articulate for the broader public the problem right now is that if there's a violation, the FTC doesn't have—may or may not have a rule specifically that's being violated and so the only thing that you can do is go to the company and say we're notifying you that you're violating Section 5 and therefore let's enter into a consent decree and then only if you violate that consent decree is there the authority to fine and so there's no real economic consequence right now for violating existing rules or statutes as they relate to privacy, which is why we need the APA authority in any law, and here comes the second question.

It seems to me absurd that we have to have the FTC come to a company, say you're violating something, then you come to an agreement, and then only if you're violating that do we get to fine

because then it becomes just a cost of doing business to, as it were, move fast and break things.

And so the question is, do you think the FTC should have the authority to fine in the first instance? I may get some qualified nos, which is fine.

Mr. CALI. A qualified no.

Mr. DEVORE. I would say subject to my prior qualified yes, it's not something that should necessarily be ruled out.

Mr. ENRIGHT. Amplifying what has been said, I would also point out that many FTC consent agreements actually do include a civil penalty as part of the settlement. So the FTC has levied financial sanctions in the first instance.

Senator SCHATZ. Right. But they're mutually agreed to. You can't just levy the fine. It has to be part of the agreement.

Mr. KIERAN. Senator, we do think that there is room for measures for accountability. By way of example, we could draw inspiration from things that are in the California legislation or even the GDPR, tying penalties to a breach notification requirement. So there's room to discuss it, but it's a qualified yes, again depending on the regulation.

Senator SCHATZ. Thank you.

Mr. TRIBBLE. We would consider that and would be happy to be involved in the discussions.

Ms. WELCH. We believe that there are rules that need to be enforced, but, again, it's a qualified yes. We just need to see the full framework.

Senator SCHATZ. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Schatz. Lots of qualified yeses and qualified nos, that makes them maybes.

I think next up is Senator Tester.

STATEMENT OF HON. JON TESTER, U.S. SENATOR FROM MONTANA

Senator TESTER. Thank you, Mr. Chairman. I want to thank you all for being here today.

By your testimony, I think you guys believe privacy is important and what's kind of interesting as I hear the conversation come on is that you're asking for some level of regulation that you can depend upon, which I think is good.

I guess the question is are you doing everything you can do now to make sure that the private information is protected, and if you're not, why aren't you? The question becomes, I guess it's in the eye of the beholder, what is private information, what's not, but the question is, is why aren't the companies doing it off the chute? Why aren't we looking to Congress to pass laws to make sure that information is kept private? Is it because everybody wants the same playing field or why is that? Can anybody answer that?

Mr. CALI. Senator, I think we are doing all we can as a company. I think there have been a lot of things that have happened this year and I think the clarity of a Federal law laying out a level playing field for all participants makes sense.

Senator TESTER. Good. So do any of you sell information that you get? I mean, I deal with most, if not all, of the companies that are

sitting at this table. Do any of you sell any of the information? No? Yes? No? Yes or no?

Mr. CALI. We do not share information without affirmative customer consent.

Senator TESTER. OK. Do you sell it if you get affirmative consent?

Mr. CALI. Affirmative customer consent, we may.

Senator TESTER. OK.

Mr. DEVORE. As I said in my opening remarks, Senator, we're not in the business of selling personal information.

Senator TESTER. So that means you don't?

Mr. DEVORE. We run a number of services that are information-dependent. So there's complexity in the answer, but there is a simple answer, which I believe is quite clear, which is we're not in the business of selling personal information.

Senator TESTER. All right. So I'm a regular guy. I'm a farmer. OK? I'm not a technology person. This thing sometimes mystifies me. OK? And I'll get on and look for a set of tires for, say, my semi truck and presto-chango, I might be checking scores on ESPN or weather on some other weather channel and up comes an advertisement for tires for my truck. How the hell do they get that information? Can anybody tell me?

Mr. ENRIGHT. So, Senator, first responding to your initial question, we do not sell personal information.

Senator TESTER. OK.

Mr. ENRIGHT. As I said in my——

Senator TESTER. So tell me how they get that information because oftentimes I do that search on Google.

Mr. ENRIGHT. Certainly. And so what you are describing is that we offer an advertising platform where we provide publishers the opportunity to monetize their content via placing advertisements that may be targeted to a user's interests, subject to that user's privacy settings, if they have not opted out of behavioral advertising.

In that situation, no personal information is passing from Google to that third party. We do not sell it nor share it in that context.

Senator TESTER. So I assume that Catherine Cortez Masto doesn't get that advertisement when she gets on the Weather Channel. So what do you classify as being personal information?

Mr. ENRIGHT. Google classifies personal information as information that would be identifiable to an individual user. So your name, your e-mail account, or——

Senator TESTER. OK.

Mr. ENRIGHT.—other information that's tied to you or your device.

Senator TESTER. So maybe it's semantics. Maybe it's something else. How do they know that that's the website? How do they know that this is the thing that they need to advertise the tires on when not everybody asks for tires on this piece of equipment?

I guess what I'm getting to is that if you're not selling information, private information, but yet you're selling information that you don't deem as private but I do and, by the way, tires are no big deal, I don't really give a damn, it's just an example, but there may be something else, like, for example, if, say, a Russian firm were to ask for that information or a Chinese firm.

Have any of you been asked for information from a firm that does business in other countries and you've given it to them or sold it to them, private or not? Any response to that? No response to that? Yes or no or just don't know?

Ms. WELCH. We don't sell personal information, Senator, and we don't sell it to foreign entities either.

Senator TESTER. OK. Same thing with everybody?

Mr. TRIBBLE. Same for Apple.

Mr. ENRIGHT. Same answer, Senator. Going back to your previous question,——

Senator TESTER. Yes.

Mr. ENRIGHT.—I want to be very clear. We understand the complexity of the Internet ecosystem——

Senator TESTER. I don't.

Mr. ENRIGHT.—and we understand that that can be intimidating——

Senator TESTER. OK.

Mr. ENRIGHT.—for a user.

Senator TESTER. For example, you're going to have to teach me how I can say no information is transferred from me because I've never seen it and if it has, it's been printed in so damn fine a print that I don't have time to read it all.

So where would that exist, for example? I don't want to pick on you. I can pick on Amazon, too, because we use you once in awhile. I use Apple, too. So I use you all.

So where would I find the information to be able to say you can't share this information with anybody, I don't care?

Mr. ENRIGHT. Well, Senator, I'm quite happy to respond to your question because we take a great deal of pride in the investments that we've made in making this as simple as possible——

Senator TESTER. I like that.

Mr. ENRIGHT.—in the Google Account.

Senator TESTER. OK. So tell me how to do it because I get on Google every day.

Mr. ENRIGHT. You can jump on to Google and search for Google Account. There will be very clear indication as to how to get to those settings and we try to make it as easy as possible.

We're also investing very heavily, leading the industry, in tools, like Your Privacy Checkup and Your Security Checkup, where we invite people into that experience so they can optimize their settings in a way that makes sense to them.

Senator TESTER. OK. I think that's good. I don't know how heavily you push that information out because I'm somebody who values my privacy, as I think most people in Montana, probably most people in this room do, and if I could say this website doesn't go anywhere else besides to my house, the information off it, I would do it every damn time, but I've never ever seen that option, to be honest with you. Maybe I'm just not paying attention.

Thank you all very much. Thank you, Mr. Chairman, for your flexibility.

The CHAIRMAN. Thank you, Senator Tester.

As a follow up to that, has Google taken any specific steps to ensure that app developers don't improperly transfer Gmail user data to the third parties?

Mr. ENRIGHT. Yes, thank you, Senator. I appreciate the opportunity to address this because I know there has been some confusing reporting on this issue specifically.

I want to make it very clear that Google does not grant third parties access to users' Gmail data. We do, however, under certain circumstances, subject to users' settings and controls, allow the user to enable third party app developers to have access to that data.

One example of this would be for a trip planning application, a user can choose, after seeing a robust privacy notice from that third party app developer, to decide to grant that app developer access to their Gmail to allow them to identify messages for things like hotel or flight reservations because the user sees utility in that, but we make that ability available to a user.

However, we have strong policies in place around all of this and if third parties abuse those policies, we will remove them from the platform.

The CHAIRMAN. Thank you.

Senator Cortez Masto.

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

Senator CORTEZ MASTO. Thank you.

Let me follow up on Senator Tester's because I think this was an important part of the conversation.

As we craft or we look to craft a Federal regulation, comprehensive, do you think it's important to identify what personal information is because everybody might identify it differently, is that correct? Would you agree or do you all agree that you all identify PII in the same way? Let's just go down the panel.

Mr. CALI. Yes, the definition of personal information would be appropriate.

Senator CORTEZ MASTO. OK.

Mr. DEVORE. Yes, Senator, I think it's critically important and it goes to the very core of protecting the most sensitive information while still enabling innovation to our customers with great products and services.

Senator CORTEZ MASTO. Right.

Mr. ENRIGHT. Agreed, Senator. Clarity and consistency in definitions would be very helpful in protecting consumers and promoting compliance.

Mr. KIERAN. Agreed. I would also add that we think it would be very important in terms of the interoperability with regional frameworks around the world that we have clarity in the United States as to the definition.

Senator CORTEZ MASTO. Yes.

Mr. TRIBBLE. Yes, clarity is very important in that definition.

Ms. WELCH. Senator, not only is clarity important but with the way that we would approach it is that we would say there shouldn't be a differentiation between sensitive and non-sensitive. It gets really hard to draw those lines and it may differ for Senator Tester versus you versus another person and so that's one way to root out some of the confusion that I think consumers are feeling.

Senator CORTEZ MASTO. Yes. I agree. The other thing that I noticed, and I think it was, Mr. Cali, you said this, was that the users' expectation of privacy is based on their using experience. I think you said something similar to that and I agree, and I think for that reason, what we are trying to do here and why we haven't been able to do it yet is it's a very difficult thing to try to put one kind of template over this idea of privacy, but one thing I do support and I'm curious, and this may have been asked, I had to step out of the room, a default opt-in. How do you feel about that? Yes or no? Would you support a default opt-in? Let's go down the panel again.

Mr. CALI. No, I don't support a default opt-in because I think it restricts the use of non-sensitive data that would restrict the benefits to consumers of daily use.

I do support an opt-in for personal identifiable information that is sensitive and where we draw that line is the question and it could be struck in any number of places.

Senator CORTEZ MASTO. OK. Thank you.

Mr. DEVORE. Your Honor, we think it's critically important to have clarity and simplicity with regard to the way our products and services work. We know that customers like services that are innovative, that work fantastically, and give them what they want, and we endeavor in every case to make it clear to customers if their data is being used, how it's being used and actually to give them concrete benefits. An example would be product recommendations as you search on the website for a particular product.

I do think that there's a concern that if you overlay a regulatory imperative like that on every interaction, you really risk breaking that kind of innovation, innovative products and services that we know customers love.

Senator CORTEZ MASTO. OK.

Mr. ENRIGHT. Echoing what was said previously, while we recognize that the most important thing in building consumer trust is preserving these notions of choice, transparency, and control in everything that we build and every product and service that we launch, we also recognize that when a user is engaging with an incredibly diverse portfolio of products and services online, much of the individual data processing is expected in connection with the normal delivery of the service that the consumer is engaging with.

So if you had individual opt-in requirements for every processing operation, you could really impair the usability of the services and disincentivize users from engaging. So we think a balanced approach is appropriate.

Senator CORTEZ MASTO. And the rest of you feel the same way?

Ms. WELCH. No, Senator. We have a different opinion about this.

We believe that a default opt-in is the right approach, that this is the best way to empower consumers and increase their confidence, and we think that that's really good for business.

If consumers believe in the services that they're participating with, that they believe their data will be protected, we think that they'll participate more and so that's the position of Charter.

Senator CORTEZ MASTO. OK. Anyone else have a different position? Please.

Mr. TRIBBLE. I'll just point out, I mean, opt-in, we think, is very appropriate in many circumstances but maybe not all.

One thing I've noticed since the GDPR came into effect, as I browse the Web, every time I turn around, I'm getting asked to approve cookies and so I think there's some risk of going overboard here and the consumer will just be—their eyes will glaze over and they'll just click on it. So I think that's an important consideration.

Senator CORTEZ MASTO. OK.

Mr. KIERAN. If I could just echo Mr. Enright's sentiments, I think it's very important to think about a practical example.

If a person comes to Twitter for the first time, we want to be able to serve them in their relevant language. We do that based on their IP address. If we had to provide opt-in consent for that, it would be very difficult and challenging.

We do, however, provide that person the ability to go back and change their location, if they choose. So that's giving them meaningful control, but as a practical matter, a default opt-in would produce difficulties.

Senator CORTEZ MASTO. Thank you. And I know my time is running out and I'll submit my questions for the record, but I do think the other thing that we need to figure out here is this idea of Federal preemption and the states' role in this space as well as the Attorney Generals' as part of it.

So thank you.

The CHAIRMAN. Thank you, Senator Cortez Masto.

Senator Lee.

STATEMENT OF HON. MIKE LEE,
U.S. SENATOR FROM UTAH

Senator LEE. Thank you very much, Mr. Chairman. Thanks to all of you for being here.

Mr. Enright, can you tell me about how much Google spent in order to comply with the GDPR?

Mr. ENRIGHT. Thank you. Senator, I don't have a specific figure available. I can tell you that for multiple years in advance of the effective date of the regulation, a massive cross-functional effort was mobilized across the company, including significant capital expenditures, in drawing time and attention of engineering and other staff toward building an appropriate compliance regime when they may have otherwise been working on products and features that users would be enjoying today.

Senator LEE. OK. Sure. And I understand it can be difficult to present an accurate estimate, but I assume from your answer, we can assume that it was more than hundreds of dollars. It was more than thousands or tens or hundreds of thousands. I assume it was certainly into the millions.

Mr. ENRIGHT. It was orders of magnitude higher than any figure that you've mentioned, sir.

Senator LEE. OK. Orders of magnitude higher than any figure I've mentioned.

And offhand, any idea on how many human hours it might have taken for Google's workforce to bring the company into compliance with the GDPR?

Mr. ENRIGHT. We do have some analysis of that that I would be happy to share with your staff, sir. I don't have those numbers available with me today.

Senator LEE. Would you estimate that it was in the thousands of hours?

Mr. ENRIGHT. I would estimate that it was in the hundreds of years of human time.

Senator LEE. Hundreds of years of human time.

Mr. ENRIGHT. Correct.

Senator LEE. OK. That is very significant and something that I think we ought to look to when we look at U.S. policy, given all the resources that it takes for a company to do that, those are racehorses that can go somewhere else. It doesn't mean that all regulations are bad. It does mean that those are things we have to take into account. Whenever we increase the size of the Federal regulatory footprint or the regulatory footprint of the states, things get significant. They end up costing consumers more money one way or another.

Federal regulations cost the American economy about $300 billion a year, 20 years ago. Today, that figure stands at about $2 trillion a year just for Federal regulations.

Mr. Cali, wanted to talk to you about an issue related to preemption. We have a lot of discussion going on on whether and to what extent Congress should preempt the playing field in this area.

Preemption necessarily turns on the scope of Federal power. As you know, the power of Congress is not limitless. We are said to be a government of limited enumerated powers and one of those powers, the power I think is probably most appropriate here, involves the power to regulate trade or commerce between the states, with foreign nations, and with Indian tribes.

One could argue that states ought to be able to regulate in this area individually. One could also argue that because the Internet itself is a channel or instrumentality of interstate commerce, it is itself subject to Congress's plenary regulatory authority, much in the same way that our interstate airways are subject to plenary regulatory authority, exclusive regulatory authority.

For instance, because we have interstate airways that are by their very nature channels of interstate commerce, even if you happen to take a flight between two cities of the same state, you're still subject to Federal regulation on that front.

How would you describe the authority in this area if Congress were to act? Is it exclusive? Is it necessarily exclusive? Is it potentially exclusive or non-exclusive?

Mr. CALI. I think it's exclusive, Senator. It's certainly good policy to treat it that way and approach it in that direction.

Always important to respect state authority. The problem is data moves at the speed of light and it doesn't respect state boundaries, and the discussion here today shows we can strike the balance in any number of ways in a given law and the problem you have is if California strikes the balance one way and New York strikes it another way and a third strikes it another way, industry will be forced because of the fragmentation to comply with the most restrictive aspects of each state's law and then we'll end up as a practical matter with a framework that is more restrictive than any

state intended and actually produces less consumer welfare than any state expected.

A Federal privacy law here, because of the nature of the Internet and the nature of these phones which travel across state lines as you talk on them, it is an interstate service and therefore should be regulated by Congress.

Senator LEE. OK. So you're saying that perhaps even more so than with respect to aviation, this is the kind of thing that by its very nature could be pragmatically difficult to impossible to administer on a state-by-state basis.

In theory, you could come up with a regulatory regime that could allow someone to take off in Northern Virginia and land in Richmond, Virginia, but it's much more difficult to contemplate something that would work as a practical matter with the Internet.

Mr. CALI. That's correct. Given the nature of the data services and the Internet and the mobility associated with it, I think it's an area of Federal regulation.

There may be areas where we need to make sure we're not intruding on state consumer protection rules, but in terms of regulating privacy for data services, I think it's essential it be done federally.

Senator LEE. Thank you. I see my time has expired. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Lee.

Senator Peters.

STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN

Senator PETERS. Thank you, Mr. Chairman, and thank you to all of our witnesses for lending your expertise to us today.

I think there's no question that consumers want better transparency and control over their personal information, which is why we're here today, and hope that we leave today with a better understanding of what a Federal privacy law might look like and how we protect consumer privacy while also making sure we're not stifling innovation in the process, as well, to allow this innovation to continue to grow because of all the benefits associated with it.

But my first question is for Mr. Enright. Through Google's Dashboard, which is reachable through your Privacy Checkup feature, you provide numerous mechanisms for users to control the collection of their data, but I'm curious about what you know about the Dashboard's effectiveness and if you could share that with the Committee.

What percentage of your users actually utilize the Dashboard?

Mr. ENRIGHT. Thank you, Senator, for the question. As I said, My Account, which is an evolution of Google Dashboard that you referenced, is an area where we are continuing to make substantial investments to ensure that we are providing the most robust set of controls to our users that we can, advancing those goals of choice, transparency, and control.

We've also, I will point out, used tools, like the Privacy and Security Checkup, to actually proactively use some of the most expensive real estate on the Internet on Google Home Page to invite users to interact with these privacy settings. We're not hiding

them. We're not obfuscating them. We are actively promoting them because we actively want users to engage with them.

Senator PETERS. So how many are using them?

Mr. ENRIGHT. I do not have specific facts and figures around numbers or percentages of users that are engaging with their privacy settings, but I could certainly produce them for your staff.

Senator PETERS. Well, we'd love to follow up with you on that because I think it's important to see how effective that is and how many folks actually realize that it's there and are able to interact with it because I know a primary concern of consumers is also how they're being tracked when they don't know it, such as when they're reading something on the Internet or how much time they're spending on various websites they may be on.

Does Google's Dashboard disclose information to your users about how you're tracking them across the Internet?

Mr. ENRIGHT. The Google Dashboard provides as much information as we are presently able about a user's use of our various products and services.

When you say track users across the Internet, what I am inferring is can a user engage through My Google to see information about ads they've seen or related information, ads they've seen as they've traversed the Internet and, yes, in fact, they can see a very robust reporting about their interaction with advertising across the Internet as it relates to Google's own ads using My Google.

They can also, I want to be perfectly clear, opt out of targeted advertising all together. If a user does not want to participate in targeted advertising, we offer a very simple control where they can turn it off with a single click.

Senator PETERS. So my question to the panel—well, first for you, Mr. Enright, but to then the panel. Would you support a Federal privacy law that mandates disclosure of that type of tracking?

Mr. ENRIGHT. Yes, Senator, we would be very supportive of legislative measures that continue to promote increased obligations for transparency and in an associated way a data portability which we think is equally important.

Senator PETERS. Any other panelists like to comment if they'd support it? I assume everybody'd support it if you're quiet.

Mr. KIERAN. We would echo those sentiments.

Senator PETERS. Everybody else would support that. Thank you.

This would also be to the panel and anyone can start with the answer.

What do you believe should be the contours of personally identifiable information? How should it be defined in Federal legislation, and how can we ensure that it will be adaptable to future advances in technology that could create new data points that would result in exposure to individuals and think facial recognition and other types of advancements that we'd see? Anybody on the panel would like to comment about how we should deal with that? I'd appreciate it. Mr. Enright, I'll start with you.

Mr. ENRIGHT. Certainly. Thank you, Senator. As to your first question, an appropriate definition for personally identifiable information, as I had said in my earlier testimony, we at Google believe that there is a logical definition for personally identifiable informa-

tion, which is data that directly identifies an individual user. Examples of this would be your name or your e-mail address.

I will point as a point of reference to the GDPR's definition of personal information, which also extends to information collected from a user, and we would say that in certain circumstances, that definition is overly broad.

So for purposes of the legislative work of this Committee, I would encourage that at least we use as a starting point the logical definition that (1) I think a reasonable consumer would infer from the phrase "personally identifiable information," which would be data elements that specifically identify an individual user.

Senator PETERS. Thank you, Mr. Enright. I'm out of time, but I'd hope to get the answers from other panelists at a future time, if possible.

Thank you.

The CHAIRMAN. Thank you, Senator Peters.

Senator Hassan.

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

Senator HASSAN. Thank you, Mr. Chair, and thanks to you and the Ranking Member for having this hearing today, and thank you to all of our witnesses for being here today.

Mr. Enright, in your testimony, you describe transparency, user control, portability, and security as Google's main privacy values.

I am disturbed, though, by reports that Google is currently working on a search engine for China that would conform with the rigid censorship requirements of the Chinese regime.

What's even more troubling is that the search engine would apparently link users' searches to their personal phone numbers, both making it easier for the Chinese Government to track and monitor its citizens and to develop their so-called social credit scores where citizens can be denied any number of things, from travel to access to school.

Fourteen leading human rights organizations have called on your company to cease its work on the search engine and a number of our colleagues, both Democrats and Republicans, have called on Google to provide additional answers to Congress, yet the company has yet to provide those answers.

How will Google square its stated privacy values with this flawed Chinese search engine and the very real possibility that it may be used to repress human rights?

Mr. ENRIGHT. Thank you for the question, Senator. First, I would like to say that I take pride in Google's record on human rights. I stand by our long track record in living by our values and launching products and services that reflect and are consistent with those values.

With that said, I am aware of the reporting that you reference and I will say that my understanding is that we are not in fact close to launching a search product in China and whether we would or could at some point in the future remains unclear.

If we were in fact to finalize a plan to launch a search product in China, my team would be actively engaged, our privacy and security controls would be followed, and any such project or product

would follow and be consistent with our values around privacy and data protection, as I've described in here today.

Senator HASSAN. So where do you think these reports are coming from?

Mr. ENRIGHT. I wouldn't speculate, Senator.

Senator HASSAN. OK. I would look forward to continued dialogue, and I think it would be in Google's interest to respond to the inquiries from Members of Congress about what kind of work you're doing with China and whether you are even contemplating building a tool that could be used by a totalitarian regime to repress human rights.

I'd like to move on now with a question again to Mr. Enright and to Mr. Kieran.

This is a really interesting panel because we have big businesses from Internet service providers to online platforms to device manufacturers and retailers all here. I hope very much that Chairman Thune and Ranking Member Nelson will host another hearing on this topic where we can also hear from consumer and public interest groups to learn even more.

One issue that I raised with Mark Zuckerberg of Facebook when he testified before this Committee is that when your companies' business models rely on maximizing the amount of time people spend on your products and monetizing people's data, it's simply not possible for us to trust that your companies will make the changes needed to protect America's well-being and privacy.

Mr. Zuckerberg committed to working with Congress to develop ways of protecting consumer and constituent privacy and well-being, even if that results in some laws that will require adjustments to your business models.

Will Google and Twitter make the same commitments here today?

Mr. ENRIGHT. Senator, we remain committed to working with this Committee and with Congress more generally as well as more broadly with legislators, regulators, and policymakers to ensure that appropriate privacy protections and data protection protections continue to exist and continue to evolve and iterate to address new and changing threats that come to face our services and users.

We believe that trust is absolutely paramount to the long-term success of our business and it's the right thing to do.

Senator HASSAN. Well, thank you for that. I want to hear from Mr. Kieran.

Mr. KIERAN. Thank you for the question, Senator. I would echo what Mr. Enright said, and I would add that at Twitter, the primary goals or objectives of the company at the moment are health and data protection privacy. We take those very seriously.

Everybody touches upon those concerns at the company. We believe they're not only key to keeping the people's trust who use our services but also showing good responsibility with respect to where our place is in the world.

We welcome the opportunity to work with you and your staff and the Committee on those initiatives.

Senator HASSAN. Well, I appreciate those answers, but I do have to tell you, and I'll look forward to following up with further questions, there is a basic disconnect here. You can be as well-intended

as possible but if your business model drives a particular set of behaviors and the monetizing of people's data, for instance, and keeping them online and your business model and your responsibility to your shareholders is one thing and the needs of the public and consumers is another thing, it may behoove you to work with us to come up with a regulatory scheme, as Mr. Zuckerberg committed to do, that removes some of that conflict because at the end of the day, if your business model is driving you in one direction, all your good intentions may not help consumers who really are demanding it.

Thank you for letting me go over, Mr. Chair.

The CHAIRMAN. Thank you, Senator Hassan.

Senator Wicker.

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

Senator WICKER. Thank you very much.

This late in the hearing, let's see if we can sort of summarize and make sure where we are with regard to the positions of all the companies you represent.

There is a fundamental principle that any Federal privacy legislation should include preemption of state data privacy laws. Do each and every one of your companies agree that our Federal legislation should include preemption? Mr. Cali, and we'll go down the panel.

Mr. CALI. Yes, I do.

Senator WICKER. Mr. DeVore?

Mr. DEVORE. Another qualified yes, Senator. The details matter a lot. I do think it's essential to avoid the risks that we've identified, which is a patchwork of state laws that have the risk of imposing regulations that don't actually serve the core interest that I think we're all focused on today, which is ensuring the customers trust the ways in which their data is being used.

Senator WICKER. Qualified yes. Mr. Enright?

Mr. ENRIGHT. Yes, Senator, we support a uniform rule of law across the country.

Senator WICKER. Mr. Kieran?

Mr. KIERAN. Yes, Senator, but I'd add for Twitter, it's not the primary reason that we're here. We do believe this law needs to balance the protection of individuals' rights with the freedom to innovate. So preemption is a part of that but it's not the——

Senator WICKER. Oh, sure. I'm going to ask about other things, too. Mr. Tribble?

Mr. TRIBBLE. As I said before, yes, assuming that it meets the bar of protecting consumers meaningfully.

Senator WICKER. And Ms. Welch?

Ms. WELCH. Yes.

Senator WICKER. OK. And do we all agree that the FTC is the place for primary enforcement of this? Mr. Cali, and on down the line.

Mr. CALI. Yes.

Mr. DEVORE. Yes, Senator.

Mr. ENRIGHT. Yes, Senator.

Mr. KIERAN. Yes, Senator.

Mr. TRIBBLE. Yes.

Ms. WELCH. Yes.

Senator WICKER. OK. And so let's talk about this issue where we might not be quite so uniform and so let me direct this to Mr. DeVore, Mr. Enright, and Mr. Kieran, whose companies are members of the Internet Association.

The Internet Association on the issue of technology and sector neutrality has called for Federal privacy legislation that is indeed technology-neutral and sector-neutral and that the legislation should include protections that are consistent for individuals across products and services and apply to online and offline companies alike.

So, Mr. DeVore, Mr. Enright, and Mr. Kieran, and we'll begin with Mr. DeVore, your companies are members of the Internet Association. Does that mean that your company believes that Edge providers and ISPs and all other online entities should be subject to the same privacy requirements?

Mr. DEVORE. Thank you, Senator. Yes, and again we believe the core principles here should apply to everyone. That's simplicity, that customers understand how their data is being used, that it's used responsibly, consistent with their expectations, and that they have ultimate control.

Senator WICKER. And Mr. Enright?

Mr. ENRIGHT. Yes, Senator, I would refer back to the Legislative Framework that we recently published and the general principles of choice, transparency, and control, which all, I think, reflect an understanding that a uniform application of a harms-based approach across industries enforced by the FTC is the right way to go.

Senator WICKER. Mr. Kieran?

Mr. KIERAN. We would echo both of those sentiments.

Senator WICKER. OK. So now let me turn to Mr. Cali and Ms. Welch.

Do you think a national privacy law should take an online entity's business model into account or should all online entities be subject to the same data protection requirements? In other words, do you differ at all with the previous three witnesses? Mr. Cali?

Mr. CALI. Senator, the information that a consumer gives to a company is sensitive or it's not sensitive, without regard to what the company's particular business model is, and the fact that we today see business models that we think are different, a business model that is a free model online, fully ad-supported versus a model that's fully supported by the subscriber, that doesn't really describe reality.

Increasingly, you're seeing hybrid models where you have a mix of subscriber payments but they're discounted because there's also ad support. So the distinction between the models also fades.

So just to repeat from a consumer perspective, it's all the same information and it's sensitive or not, and then from a model perspective, we have a mix of models in the market.

Senator WICKER. OK. Well, can I get a yes or no? Do you agree with the Internet Association's position with regard to this issue?

Mr. CALI. I agree that it should be—yes, I do, consistent.

Senator WICKER. OK, OK. And Ms. Welch, you have the last word.

Ms. WELCH. Yes.

Senator WICKER. OK. And my time has just expired. Thank you very much.

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 the Chairman for having this hearing and also thank him for mentioning a potential second hearing involving the European Union GDPR officials and advocate from California and public interest groups.

I think that public interest groups particularly play an extremely important part in this conversation. They were successful in California and in Europe and I want to also express my appreciation for all of you for being forthcoming in meetings with me and my staff as well as your being here today, not to mention your tremendous contribution to our economy, to quality of life, to so many aspects of American consumers.

Let me just sort of establish some first principles. Does anyone here believe that Americans deserve less privacy than Europeans? If you do, raise your hand.

[No response.]

Senator BLUMENTHAL. The record will reflect no hands were raised.

Do any of you believe that all Americans deserve less privacy than Californians will have under the new law going into effect there?

[No response.]

Senator BLUMENTHAL. Again, no hands raised.

So many of you have been critical of the GDPR and some of you, let me be very blunt, fought the California law. That's a matter of public record.

I am really seeking assurance that you will put your money where your mouth is and I recognize that we are talking here about monetizing an asset which is consumer information. Your companies have lots of it and they are a principal means of profit-making, and I guess my first question or my next question for you is, do all of you agree that Congress cannot settle for voluntary practices or self-regulation? Do all of you agree that we need mandatory practices and rules of the road when it comes to privacy?

Again, no apparent dissent from that point of view.

Because voluntary rules have just proved insufficient to protect privacy, and I guess my question is why should we not simply then adopt here the same standards that are going to prevail in California, which are also consistent with the standards in Europe regarding minimization and consent and the general respect for consumers that those two sets of rules embody?

I think that question lingers here. It will linger after this hearing. I recognize that your answers may be complex and lengthy and therefore we don't really have the opportunity to explore all of

those answers here, but I really hope that you will be at the table sincerely seeking to frame answers that protect American consumers and so let me just open it to you to two final questions.

Anybody here planning to pull out of Europe because of those privacy protections, any of your companies?

[No response.]

Senator BLUMENTHAL. No one. So you're living with them. No undue hardship.

Any of you planning to pull out of California?

[No response.]

Senator BLUMENTHAL. Again, no one. No undue hardship.

So what that tells me is that the opposition that you've expressed to these rules, recognizing that the devil may be in the details, is one that can nonetheless accommodate the kinds of rules that we have seen in the GDPR and in California, correct?

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal.

Senator Markey.

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

Senator MARKEY. Thank you, Mr. Chairman.

The reason we're here is that Europe has now passed a privacy law and California has passed a privacy law. At the end of the day, the companies which are represented here today and all across the country are ultimately going to want California law preempted and they're going to want other states' laws preempted. They're going to ask this panel to do that.

So our goal has to be to ensure that any law which we pass out of this committee is a strong law, and we don't need to pass weak laws in Washington that override strong laws in California or Massachusetts or other states. So that's why we're here because finally Europe, finally states are beginning to move in the absence of a Federal policy but that Federal policy is going to have to be strong.

The bill which I've introduced for years, which is essentially the Consent Act, basically says (1) people should have a right to knowledge that information is being gathered about them, (2) notice that that information might be reused for purposes that they never intended it to be used, and (3) that they have a right to say no, that they don't want it to be reused.

So, Mr. Kieran, I can begin with you. Would Twitter support a Federal privacy bill that requires companies to tell consumers in a clear and concise way what information is being collected about them and how that information is being used, shared, retained, or sold?

Mr. KIERAN. Yes, Senator. Twitter already has those practices in place. We believe it's paramount to keeping the trust of the people that use our services and we would support that type of legislation.

Senator MARKEY. Would each of the other companies which are here support a provision which provides that level of information transparency with your consumers? Mr. Cali?

Mr. CALI. Yes, we very much believe in transparency and giving customers' choice.

Senator MARKEY. Thank you, sir. Mr. DeVore?

Mr. DEVORE. Yes, Senator.
Senator MARKEY. Mr. Enright?
Mr. ENRIGHT. Yes, Senator.
Senator MARKEY. Thank you. Mr. Tribble?
Mr. TRIBBLE. Yes.
Senator MARKEY. Ms. Welch?
Ms. WELCH. Yes, Senator.
Senator MARKEY. Thank you. Of course, requiring transparency is a good first step but we then have to move on to the question of the right of a consumer to say no, they don't want the information to be shared with anyone else, other than the company with which they have been engaging in that relationship, that transaction.
Mr. Enright, should a Federal privacy policy establish consumers' right to control their personal information and give consumers the right to say no to their data being sold or shared with others?
Mr. ENRIGHT. Yes, Senator.
Senator MARKEY. Yes. Mr. Cali, do you agree?
Mr. CALI. Yes, I do, and I would like to just correct. I was informed I may have misspoken earlier.
Our policy very clearly says through the AT&T Communications Company we do not sell personal information and we reserve the right to share it, not sell it, with affirmative customer consents.
Senator MARKEY. OK. I just want to keep going down the line on this question.
Mr. Enright, just answer. Do you agree, Mr. Enright, with Mr. Cali?
Mr. ENRIGHT. Yes, yes.
Senator MARKEY. Mr. DeVore?
Mr. DEVORE. Yes, Senator.
Senator MARKEY. Mr. Kieran?
Mr. KIERAN. Yes, Senator.
Senator MARKEY. Mr. Tribble?
Mr. TRIBBLE. Yes.
Senator MARKEY. Ms. Welch?
Ms. WELCH. Yes, Senator.
Senator MARKEY. Ms. Welch, having control of information also means having access to it. Should Americans be able to access their personal data online, would Charter support a Federal policy bill that would enshrine that right into law?
Ms. WELCH. Yes, Senator.
Senator MARKEY. Mr. Cali?
Mr. CALI. Qualified yes.
Senator MARKEY. Mr. DeVore?
Mr. DEVORE. Yes, Senator.
Senator MARKEY. Mr. Enright?
Mr. ENRIGHT. Yes, Senator.
Senator MARKEY. Thank you. Mr. Kieran?
Mr. KIERAN. Yes, Senator.
Senator MARKEY. Mr. Tribble?
Mr. TRIBBLE. Yes, Senator
Senator MARKEY. Thank you. And Ms. Welch, thank you.

Well, we have the beginnings of something here, although we'd have to come back to spend a little more time over here with Mr. Cali and AT&T, which we're time-limited.

I just want to ask one quick question of Mr. DeVore. Recently, Amazon's facial scanning technology recognition misidentified 28 Members of Congress, including me and Congressman John Lewis. I wrote a letter to Amazon about those issues. I don't think it quite answered all of my questions but I just quickly ask you.

Can Amazon's facial recognition technology determine whether it is taking pictures of children under 13 and how does Amazon ensure that recognition, your product, is compliant with the Children Online of Privacy Protection Act?

Mr. DEVORE. Thank you, Senator. To be really clear, that technology doesn't take any pictures at all. It's just a matching technology and it's dependent entirely on the dataset that a customer that's using the technology uses in connection with the service.

So it doesn't take pictures. It has a number of uses. It just matches photos and videos and objects, entirely dependent on the dataset provided.

Senator MARKEY. And the problem, of course, is that it matched me and Congressman Lewis and wound up putting me into a suspicious category and so have you tested it for any biases related to race or gender to ensure that that is not going to be a part of the product at the end of the day?

Mr. DEVORE. Senator, we have tested it. We are an innovation company. We're constantly improving the product. We have also replicated the study that the ACLU reported and were not able to replicate those results with a much, much larger dataset.

So we think there are flaws in the study. We have engaged with the ACLU to try to understand better what they did.

Senator MARKEY. And I look forward to working with Amazon and all of you toward putting together a strong national privacy bill before we discuss preemption of state laws.

Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey.

Senator Udall.

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

Senator UDALL. Thank you very much, Mr. Chairman, and appreciate the witnesses being here and, Senator Markey, I'm going to follow up on some of your COPPA questions there since I know you were a big sponsor and passed COPPA in 1998 and I think it went into effect in 2000.

This summer, I sent letters to Google, its subsidiary YouTube, MoPub, a subsidiary of Twitter, and Tapjoy, raising concerns about their compliance with the Children's Online Privacy Protection Act, known as COPPA.

Mr. Chairman, I'd ask unanimous consent to add these letters to the record.

The CHAIRMAN. Without objection.

Senator UDALL. Thank you.

[The letters referred to follow:]

UNITED STATES SENATE
Washington, DC, September 25, 2018

SUNDAR PICHAI,
Chief Executive Officer,
Google,
Mountain View, CA.

Dear Mr. Sundar Pichai:

I write regarding the Google Play Store's compliance with the Children's Online Privacy Protection Act (COPPA). As one of one two major mobile operating systems, Google has a responsibility to ensure apps on the Android Platform follow U.S. Jaw to protect children's privacy online. I urge you to direct an audit of all applications in the "Designed for Families" section of the Play Store to ensure compliance with COPPA, remove any app that violates the law, and improve app vetting in this section going forwards.

COPPA protects children from being improperly tracked including for advertising purposes. It explicitly prohibits children's apps from collecting personal details including names, e-mail addresses, geolocation data and tracking identifiers like advertising identifiers. The "Designed for Families" section, as well as the age-appropriate rating, misleads parents to believe that Google ensures that these apps are compliant with COPPA.[1]

According to a Proceeding on Privacy Enhancing Technologies Study, nearly half of the 6,000 free children's Android apps are potentially in violation of COPPA.[2] This report of thousands of apps are potentially illegally tracking children is worrisome.[3] American families should have a reasonable expectation of privacy for their children when they use the Android platform and that apps available in the families section do not violate COPPA. Given the potential for COPPA violations, I respectfully ask Google to answer the following questions about its efforts at compliance:

- What specific steps does Google currently take to ensure that apps in the "Directed for Families" section are abiding by your tenns of service with regards to COPPA?
- How do you currently audit the "Designed for Families" section?
- In the last year, how many applications have you removed from the Google Play Store due to violations of COPPA? If so, please provide all details regarding app, date, and cause for action.
- Of those applications in the "Designed for Families" section, how many send personally identifiable information about children to third-party applications without verifiable parental consent?

Thank you for your attention to this important issue. Please provide a written response no later than Monday, October 22, 2018.

Sincerely,

TOM UDALL,
United States Senator.

---

[1] Valentino-De Vries, 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*

[2] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman (2018) "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing. Technologies.* 2018 (3), 63-83. *https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf*

[3] Shaban, Hamza. "Thousands of apps in Google Play Store may be illegally tracking children, study finds." *The Washington Post.* 2018, April 18. *https://www.washingtonpost.com/news/the-switch/wp/2018/04/16/thousands-of-android-apps-may-be-illegally-tracking-children-study-finds/*

UNITED STATES SENATE
Washington, DC, September 25, 2018

Hon. JOSEPH SIMONS,
Chairman,
Federal Trade Commission,
Washington, DC.

Dear Chairman Simons:

I write to express concerns about "kid-directed" mobile apps potentially violating the Children's Online Privacy Protection Act (COPPA) and urge the Federal Trade Commission (FTC) to conduct an investigation and take any necessary corrective actions.

As you know, COPPA protects children from being improperly tracked, including for advertising purposes. It explicitly prohibits children's apps from collecting personal details including names, e-mail addresses, geolocation data and tracking identifiers like advertising identifiers. The "Designed For Families" section of the Google Play Store, as well as the "Kids" section of the Apple App Store, leads parents to believe that Google and Apple, respectively, ensure that these apps are compliant with COPPA. There is now increasing evidence that this is not the case. Combined, These two app platforms reach the overwhelming majority of U.S. consumers, including children.

As part of any investigation, FTC staff should review the Proceeding on Privacy Enhancing Technologies Study, which found that nearly half of the 6,000 free Android apps that are "Designed for Families" are potentially in violation of COPPA.[1] In addition, recent press reports also indicate that thousands of apps in the "Designed for Families" section of the Google Play Store are potentially illegally tracking children's online activities.[2] An analysis done by the New York Times also found that children's apps in both the Apple App Store and the Google Play Store sent data to tracking companies, potentially violating COPPA.[3]

In light of these troubling signs of lack of compliance, I urge the FTC Launch an investigation of both the Android and Apple platforms to determine whether apps in the "Designed for Families" section of the Google Play Store or the "Kids" section of the Apple App Store are violating COPPA, and if so, quickly take the necessary corrective actions.

Unbeknownst to parents, it appears that many of these apps are sharing information like mobile advertising ID and hardware persistent ID with third-party analytics and advertising platforms. I have already sent letters to some of the advertising networks that have been implicated the Proceeding on Privacy Enhancing Technology Study asking them to ensure that their software is not being used by any apps in the "Designed for Families" section of the Google Play Store. As the FTC is the major governing body tasked with enforcing COPP A, I urge the FTC to investigate these apps to ensure that the law is being followed.

Additionally, as the FTC is undertaking a series of hearings on large online platforms implications for competition, I urge you to include a separate hearing on the impacts that those platforms and technology are having on children—either through connected devices, targeted video content, or activity online. While I strongly support COPP A, I believe that it is time for the FTC to work with privacy experts and Congress to outline ways to improve and modernize the law.

Thank you for your prompt attention to this important matter. We look forwards to FTC's renewed efforts to ensure that children's privacy is protected in this increasingly digital world.

Sincerely,

TOM UDALL,
United States Senator.

---

[1] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman (2018) "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing. Technologies.* 2018 (3), 63-83. *https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf*

[2] Shaban, Hamza. "Thousands of apps in Google Play Store may be illegally tracking children, study finds." *The Washington Post.* 2018, April 18. *https://www.washingtonpost.com/news/the-switch/wp/2018/04/16/thousands-of-android-apps-may-be-illegally-tracking-children-study-finds/*

[3] Valentino-De Vries, 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*

UNITED STATES SENATE
Washington. DC, August 24, 2018

STEVE WADSWORTH,
Chief Executive Officer,
TapJoy,
San Francisco, CA.

Dear Mr. Wadsworth:

We write due to our concerns with recent reports that TapJoy is collecting personally identifiable information about children without verifiable parental consent.[1] According to a Proceedings on Privacy Enhancing Technologies study, TapJoy is among the most common destinations for data gathering that appears to vio late the Children's Online Privacy Protection Rule (COPPA).[2] As a mo bile advertising platform, TapJoy has an added duty to ensure that children under 13 are not targets of behavioral advertising.

The research found evidence that mobile apps were sending to Tap.Toy the personally identifiable information of children, such as Device ID, e-mail or MAC address without parental consent. While TapJoy purportedly prohibits the use of its service for apps directed towards children under 13, over a hundred kid-directed applications with 386 million downloads use your software development kit. We urge you to review kid-directed apps on the Google Play Store that use your platform to ensure compliance with COPP A. Additionally, we urge you to build configurations to ensure compliance with COPPA.

Because TapJoy serves apps that may serve children, COPPA requires the company to take precautions to protect children's privacy.[3] Congress passed COPPA in 1998 to protect children's privacy by providing parents with tools to control the info rmation collected online about their children ages 12 and under. While use of TapJoy by kid-directed application is against the terms of service, it is clear that there are many kid-directed applications on the Google Play Store using the TapJoy platform in violation of those terms. We ask that you rescind service from any applications in the kid-directed section of the Google Play Store which use your advertising service.

We want to ensure that children's privacy is respected and that advertisers don't violate existing federal law by inappropriately targeting them. We respectfully ask that you answer the following questions:

- How many applications in the kid-directed section of the Google Play Store use the services ofTapJoy?
- Of those applications, how many send TapJoy personally identifiable information about children?
- What types of personally identifiable information about children do you receive from applications? How do you use that information? With whom do you share that information, and for what purposes?
- How do you or your partners use personally identifiable information about children to target children with advertising?
- What specific steps does TapJoy currently take to ensure that child-directed applications are not using TapJoy, and to ensure that mobile applications using TapJoy are abiding by your terms of service with regards to COPPA?
- Have you ever rescinded service to an app due to COPP A violations or related violations of your terms of service? If so, please provide all details regarding app, date, and cause for action.

---

[1] Shaban, Hamza. "Thousands of apps in Google Play Store may be illegally tracking children, study finds." *The Washington Post.* 2018, April 18. *https://www.washingtonpost.com/news/the-switch/wp/2018/04/16/thousands-of-android-apps-may-be-illegally-tracking-children-study-finds/*

[2] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman (2018) "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing. Technologies.* 2018 (3), 63-83. *https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf*

[3] Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2003).

Thank you for your attention to this important matter. Please provide a written response no later than September 28, 2018.

Sincerely,

TOM UDALL,
United States Senator.

MARGARET WOOD HASSAN,
United States Senator.

UNITED STATES SENATE
Washington, DC, August 24, 2018

JACK DORSEY,
Chief Executive Officer,
Twitter,
San Francisco, CA.

Dear Mr. Dorsey:

We write due to our concerns with recent reports that Twitter subsidiary, MoPub, is collecting personally identifiable information about children without verifiable parental consent.[1] According to a *Proceedings on Privacy Enhancing Technologies* study, MoPub is among the most common destinations for data gathering that appears to violate the Children's Online Privacy Protection Rule (COPPA).[2] As a mobile advertising platform, MoPub has an added duty to ensure that children under 13 are not targets of behavioral advertis ing.

The research found evidence that mobile apps were sending to MoPub the personally identi fiable information of children, such as Device ID, e-mail or MAC address without parental consen t. While MoPub purportedly prohibits the use of its service for applications directed towards children under 13, 148 kid-directed apps with 296 million installations use your software development kits. We urge you to review child directed applications on the Google Play Store that use your platform to ensure compliance with COPPA. Additionally, we urge you to build configurations to ensure compliance with COPPA.

Because MoPub may serve applications that serve children, COPPA requires the company to take precautions to protect children's privacy.[3] Congress passed COPPA in 1998 to protect children's privacy by providing parents with tools to control the information collected online about their children ages 12 and under. While this is against the terms of service for MoPub, it is clear that there are many kid-directed applications on the Google Play Store using the platform in violation of those terms. We ask that you rescind service to applications in the kid-directed sectio n of the Google Play Store which use MoPub.

We want to ensure that children's privacy is respected and they are not being inappropriately targeted by advertisers according to the laws passed by Congress. We respectfully ask that you answer the following questions:

- How many applications in the kid-directedsection of the Google Play Store use the service of MoPub?
- Of those applications, how many send MoPub personally identifiable information about children?
- What types of personally identifiable information about children do you receive from applications? How do you use that information? With whom do you share that information, and for what purposes?
- How do you or your partners use personally identifiable information about children to target children with advertising?
- What specific steps do you currently take to ensure that child-directed applications are not using MoPub, and to ensure that mobile applications using either serviceare abiding by your terms of service with regards to COPPA?

---

[1] Shaban, Hamza. "Thousands of apps in Google Play Store may be illegally tracking children, study finds." *The Washington Post.* 2018, April 18. *https://www.washingtonpost.com/news/the-switch/wp/2018/04/16/thousands-of-android-apps-may-be-illegally-tracking-children-study-finds/*

[2] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman (2018) "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing. Technologies.* 2018 (3), 63-83. *https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf*

[3] Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2003).

- Have you ever rescinded service to an app due to COPPA violations or related violations of either terms of service? If so, please provide all details regarding app, date, and cause for action.

Thank you for your attention to this important matter. Please provide a written response no later than September 28, 2018.

Sincerely,

TOM UDALL,
United States Senator.

MARGARET WOOD HASSAN,
United States Senator.

Senator UDALL. Mr. Chairman, this committee needs to devote considerable resources and focus on policy to protect children's online privacy. We need to hold a separate hearing on what a future framework that protects children should look like.

I mentioned Senator Markey's efforts on COPPA. The Internet and our children's online activity look very different than when COPPA was passed. We didn't have Facebook or Twitter or social media. Our Internet activity was not surreptitiously tracked. We couldn't imagine we would have speakers connected to the Internet in our homes or in our kids' bedrooms. Our laws protecting children's privacy need to keep pace with the technology.

Each one of your companies has said publicly or privately that we must push through Federal legislation based on a framework that preempts states from passing their own protections, and I'm here to say we cannot push through a weak Federal law that preempts states and leaves consumers, especially children, without the necessary safeguards and protections.

We must have strong enforceable laws and we must continue our partnership with states' Attorneys General who I know from having served as New Mexico's Attorney General have their ear to the ground and receive a tremendous amount of input from consumers.

Now there are a number of public reports that strongly indicate that there are thousands of apps aimed at children that violate COPPA by tracking their online behavior.

Do we all agree that this is a potentially serious problem deserving of our collective attention? Yes or no down the line?

Mr. CALI. Yes, Senator.

Mr. DEVORE. Yes, Senator.

Mr. ENRIGHT. Yes, Senator.

Mr. KIERAN. Yes, Senator.

Mr. TRIBBLE. Yes, Senator.

Ms. WELCH. Yes, Senator.

Senator UDALL. Thank you. Now, Mr. Enright and Mr. Tribble, Google and Apple dominate the mobile operating system. As such, they are tasked with ensuring that kid-directed apps on both platforms comply with COPPA.

A recent *New York Times* analysis found that both platforms have apps in their respective children's or family sections that may potentially violate COPPA.

What specific action does each of your companies take to verify compliance with COPPA in either the App Store or the Google Play Store, respectively? Mr. Enright, Mr. Tribble, please.

Mr. ENRIGHT. Thank you, Senator, and I'd like to thank you for your leadership in drawing attention to this important issue.

Protecting children online is a top priority for Google. In connection with the App Store, we actually created a Design for Families Program to help identify applications that are kid-directed.

We require that third party developers that submit applications to the App Store identify whether in fact their applications are intended for children and, if so, they represent that they comply with the Children's Online Privacy Protection Act and other applicable legal requirements.

If we become aware that they've violated those requirements, then they are removed from the Play Store.

Senator UDALL. And do you agree that the studies and the reporting out there show that there are major violations of COPPA?

Mr. ENRIGHT. We rely upon the developers themselves to identify whether or not the content is child-directed. We think that the developers are in the best position to do so rather than us as the platform operator, but we remain committed to doing all that we can to protect children when they're using our services.

Senator UDALL. Thank you for that answer. Mr. Tribble?

Mr. TRIBBLE. Yes, we are committed to protecting children when they use our service, and with respect to our App Store, we have very strict guidelines ourselves consistent with COPPA, and we review every single app before it goes into the store. We review the apps before they get updated and if we get credible information when an app is out there in the store that it has a problem, we will take action and remove it from the store.

Senator UDALL. Just in summary and I thank you, Mr. Chairman, for the courtesies just a second here, I think this is a very serious problem, and I think that any of you that would like—I'm out of time—to answer the question or the issues that I've raised on the record, I'd appreciate that, but I hope, Chairman Thune, that we can look into this because the record seems to be that there's a lot of violation of COPPA across the board, not necessarily just from these companies but other subsidiaries and others that are operating out in this space.

Thank you.

The CHAIRMAN. Thank you, Senator Udall, for raising that and keeping it in front of the Committee's attention.

Senator Gardner.

STATEMENT OF HON. CORY GARDNER,
U.S. SENATOR FROM COLORADO

Senator GARDNER. Well, thank you, Chairman Thune, and thanks to the witnesses for your time and testimony today.

Mr. Tribble, on one hand, I was pleased to see recent a news article that highlighted Apple's decision to use the Taiwan flag, the Taiwan's flag and the name Taiwan in your latest product release last week.

On the other hand, however, Apple has previously furthered China's anti-Taiwan propaganda, including through its software. For example, news reports reveal that Taiwan's flag emoji was not accessible for IOS users located in Mainland China. This follows other instances of complying with Chinese demands, including removal of VPN apps on the App Store, forced data localization, and

the potential for Chinese Government access to sensitive personal information about dissidents and ethnic minorities.

Does Apple consider the safeguarding of human rights and protection against government oppression when developing your software?

Mr. TRIBBLE. Thank you, Senator. We make our products for customers, not countries, and our values and beliefs, including privacy and security, don't change from country to country, and the privacy is one of our central values.

This is why we apply practices to protect our customers in China and throughout the world. We make sure——

Senator GARDNER. I'm going to have to cut you short because I'm going to try to get through a lot here. Are those principles in the process for their consideration formalized and public?

Mr. TRIBBLE. Well, we have a major section of our website that goes through our privacy principles and examples of how we employ those principles.

Senator GARDNER. Mr. DeVore, Amazon maintains operations in Mainland China, albeit in limited manner in accordance with Chinese law.

Do you believe Amazon is operating under the same circumstances today that the company expected to operate under when you entered China several years ago?

Mr. DEVORE. No, Senator.

Senator GARDNER. Has Amazon relinquished full control of its cloud-based assets in China in order to comply with recent changes to Chinese law and, as a result, does a particular Chinese company now have access to all related data Amazon previously stored and maintained on those assets in China?

Mr. DEVORE. Thank you, Senator. The answer to that question is also no.

Senator GARDNER. To both those questions?

Mr. DEVORE. I'm sorry?

Senator GARDNER. To both questions?

Mr. DEVORE. That's right.

Senator GARDNER. Relinquished full control, the answer is no,——

Mr. DEVORE. That's right.

Senator GARDNER.—and no company in China has access to all related data Amazon previously stored and maintained on those apps that's in China?

Mr. DEVORE. Just to be very clear, so we're absolutely committed to security, particularly of our direct cloud products.

In order to operate in China, we are required by Chinese law to operate through a 100-percent-owned Chinese subsidiary. So it does function——

Senator GARDNER. And that Chinese subsidiary does not have data Amazon previously stored and maintained on those assets in China?

Mr. DEVORE. Just very simply, the way the AWS services work is that they're there for the customer, the entirety of the products and services. So the customer gets an instance and they have control over that instance and the data.

Senator GARDNER. The Chinese Company does?

Mr. DEVORE. No, no. The customers do.

Senator GARDNER. OK. And so the Chinese company does not have any access to that data?

Mr. DEVORE. The way the system is built, it's designed to give customers absolute control over their data. Structurally, that's the way it works at Amazon.

Senator GARDNER. So the Chinese doesn't——

Mr. DEVORE. As I mentioned, the structure of the business in China is different.

Senator GARDNER. So we can talk about that further, but you're saying that they—the answer is no, the data previously—Amazon previously stored is not in the hands of that 100-percent Chinese-owned company?

Mr. DEVORE. I'll try to be as clear as I can, Senator. The way that the system works is that data is actually controlled by the individual customers. That's the premise of the operation. The company is structured differently in China and so we are operating in China through the subsidiary that I identified.

Senator GARDNER. We'll continue that, if we could, outside the hearing.

Mr. Enright, Google made headlines in 2010 when the company made the decision to withdraw its search engine services in China rather than comply with new Chinese censorship laws.

Recent news reports, however, indicate that Google may be rethinking that decision. I understand you're unlikely to comment on those reports today, but you joined Google in 2011, shortly after that decision.

In a 2015 speech at the International Association of Privacy Professionals event in Singapore, you said that the Asia Pacific Region was on the cusp of a tremendous opportunity to build a set of privacy laws and regulations that could foster "economic, social, and public benefits that can be realized from data and data-driven technologies."

Since you joined Google in 2011 and since that 2015 speech, do you believe that China's privacy laws and regulations have shifted in a direction that fosters such greater global engagement and economic opportunity?

Mr. ENRIGHT. Thank you, Senator. I have not seen legislative or regulatory developments in China that I think would fundamentally shift my assessment.

Senator GARDNER. So the answer is no. The answer is no. Thank you.

In that same speech, you said that your trips to places, including Beijing and Shanghai, "established a commitment that my team and I would always remain closely engaged with our Asian colleagues to ensure that the evolution of Google's Privacy Program would remain sensitive to and informed by the perspectives from these important markets."

Could you explain to the Committee what you meant when you said that Google's Privacy Program would remain sensitive to perspectives from countries like China who are major markets in the Asia Pacific Region?

Mr. ENRIGHT. Yes, Senator. Consistent with my prior remarks and with my remarks at the event you reference in Singapore and

consistent with our values as an organization where right from our founding mission to organize the world's mission and make it universally accessible and useful, we design and launch products with an eye toward making the benefits of technology available as broadly around the world as we can. Expansion in APEC generally, in the Singapore market and in other areas where I was speaking, remains important.

That said, as I had said earlier, I'm not aware of any plans that we are near to launching or close to launching a search product in China nor do I think that we could or would launch a product without having our privacy controls thoroughly engaged, our Privacy Program actively involved, and any product that we launch anywhere in the world is going to reflect our values and the commitments that we've made to our users.

Senator GARDNER. Mr. Enright, I'm very concerned about how people in China and other places where there are oppressive regimes will have access to technology that may change their lives, shift their lives when millions of people are imprisoned in political camps, internment camps, re-education centers because of their minority status or because of their religion. Churches are being bulldozed.

I think it's very important that we have an open Internet and that we continue that and that we use this great tool of freedom and democracy around the globe and we have those values in the U.S. available to humans around the globe to provide and promote human dignity.

Countries like China present major market opportunities for U.S. companies. I understand that. It's important to gain a foothold, boost revenue and compete against other national companies, particularly those owned by China, but countries like China also have records littered with cracking down on dissidents, moving the goalposts for companies locating in their countries, stifling free speech, and perpetrating human rights abuses against their own citizens.

So American technology companies interested in growth abroad continue to find themselves in this very unenviable position of either having to defy local laws or having to provide hostile governments' access to sensitive and personal information about their own citizens.

Make no mistake, countries like China are already forcing companies, as we've heard today, to make these decisions and as we've heard from many of you on this panel, for decades, the U.S. has been shown as a beacon of democracy, opportunity across the world.

American companies help us carry that banner and those values to every corner of this globe, and I hope we can continue to work with all of you to discuss the challenges that we've covered today to tackle these challenges and make sure that we get back to the day that our values carry the day as the world decides whether the path to prosperity runs through China or runs through the United States.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Gardner.

Senator Baldwin.

STATEMENT OF HON. TAMMY BALDWIN,
U.S. SENATOR FROM WISCONSIN

Senator BALDWIN. Thank you, Mr. Chairman.

It's been a very informative hearing, and I hope the first of many to come. I would associate myself with the comments of other Senators that we hear some additional perspectives in future hearings on data privacy, including consumer and privacy advocates of the states and other types of entities.

But thank you all for being here to testify today. Every day, Americans share enormous amounts of personal information with a broad array of companies, including hardware, software, and certainly retailers, and doing so has become just a central part of our every-day lives, and it provides tremendous benefits to us, but it also becomes so commonplace that I think many do not fully understand what data that they may sharing and we've seen too many companies fail to keep that data secure or ensure that it's used for the purposes that their customers expect.

I want to start, Mr. Tribble, after it was revealed that Cambridge Analytica obtained millions of Facebook users' data without their knowledge or permission, Apple's CEO, Tim Cook, suggested in the press that Facebook's business model, providing a free service supported by monetizing user data, carries different data privacy risks than that of a company that sells products or services to customers.

I think there's a broad agreement that the same data privacy standards should apply to a range of actors in this sector, but as we look at the potential Federal legislation around data privacy, how should we take into account incentives around treatment of user data that may or may not exist, depending on the business model?

Mr. TRIBBLE. Thank you, Senator. Well, Apple's business does not depend on collecting customers' information. It's not our lifeblood.

Nonetheless, I believe that any comprehensive legislation should apply equally to companies because, you know, almost any company in operation today is going to at some point touch customer private information or personal information. So I think there should be an even playing field. Everyone should be subject to comprehensive Federal regulation in that respect.

Senator BALDWIN. And, Mr. Enright, as a company that also offers free services to consumers, what's Google's perspective?

Mr. ENRIGHT. Thank you, Senator. I think it's important to point out that Google's business model is predicated on the trust of our users. If our users don't trust us with their data, our long-term success is in peril.

I would also point out that many companies, both those testifying here today and elsewhere, rely upon things like ads and search for their business models to work, as well, and I think it's encouraging to hear from the testimony today that there seem to be shared values of choice, transparency, and control, and I agree that if we can begin from those first principles, continue the discussion looking at inputs, like the Legislative Framework that we recently published, we should be able to find a shared understanding and a shared direction for uniform legislation to protect consumers.

Senator BALDWIN. I'm hoping to fit in two additional questions here.

In terms of commitment to transparency about what you do with the data of your customers, I want to clarify whether any of you would distinguish between data that a consumer knows they give you or data that she may not know that she is providing. For example, websites she visits or her locations. Does anyone distinguish between those? Mr. Cali?

Mr. CALI. I don't believe so, if I understand the question. We treat information, if it's personally identifiable or not, and personally identifiable information includes information a customer gives us or information we observe, it can. So there's no distinction in that regard.

Senator BALDWIN. OK. Mr. DeVore?

Mr. DEVORE. Senator, we endeavor to take great care of customers' information, no matter what, and we really think about it not in terms of data but in terms of customers and trying to delight customers with our products and services in a way that they understand how their data is being used that provides great value to them and in best case delights them with the way the products and services work.

Different data, I think, should be protected more when it's more sensitive or when it's used in a sensitive way and that's what I would think about protecting customer trust in connection with everything we do.

Senator BALDWIN. So you do make those distinctions, it sounds like. Mr. Enright?

Mr. ENRIGHT. Consistent with the general principles of choice, transparency, control that we've described, while I do recognize that the way that we treat consumer information should be proportional to the level of risk associated with that information, I think more generally in response to your specific question, we should recognize that there is an obligation across industries to invest heavily in consumer education and consumer awareness so that users really do understand the kinds of information collection and use that is involved with the various services within which they're engaging and, similarly, invest in improved controls and awareness of those controls so that we put users back in the driver's seat and they remain in control of how companies are using information from and about them.

Senator BALDWIN. Mr. Kieran?

Mr. KIERAN. Senator, we don't differentiate between the data. We largely have sort of three blocks of data that we receive at Twitter. So there's sort of a public data that we receive from you when you use our service, so whether it's a tweet or a retweet or favorite or a like. There's the information that we need when we are operating the service. That might be things like your IP address to serve it to you in the right language and other information that we might get about your device, and then there's a third bucket, which is sort of the consent-based where it's information that if you want us to customize the service to your likings, we'll get your consent for it, but we're very transparent in those types of individual buckets.

We provide users the ability to both see it through a dashboard but also to download a copy of it, but we do treat it all in a similar fashion in terms of transparency and control.

Senator BALDWIN. Mr. Tribble?

Mr. TRIBBLE. Senator, we go through great efforts to explain to customers how we're collecting and using their data, but we don't differentiate data based on whether they understand that or whether they know that the data is being collected at the end of the day.

Senator BALDWIN. Ms. Welch?

Ms. WELCH. Senator, we also focus on the personal information of the customer and make sure that we're protecting that, and we believe any future framework should likewise empower the consumer to really have an affirmative choice about how their data is used.

Senator BALDWIN. Mr. Chairman, I know I've run out of time. I just want to put a question out there for the record and I'll follow up with the witnesses later.

But just sometimes it's hard for me to figure out if we are talking about data security or data privacy or both, and this hearing has focused on data privacy, but I'm wondering if our witnesses think we have an adequate way of drawing a line that distinguishes between the two.

When I think about—I have expectations of both security of my data as well as privacy and sometimes that is a very gray area.

The CHAIRMAN. They're used interchangeably. Well, that's a good question for the record. We'll look forward to having it.

Senator BALDWIN. Yes. I mean, there's a difference between a hack and a breach and sale of it, and where there are expectations that the Congress of the United States might act on both, should we do so in one bill or two bills or multiple?

Anyways, it creates a lot of interesting additional dialogue that we don't have time for at this moment.

The CHAIRMAN. We've been trying to solve the data security issue for a long time, so far without success. So maybe coupling it with data privacy will get us there. We'll see, but these hearings are helpful in that regard.

Senator Cruz.

STATEMENT OF HON. TED CRUZ, U.S. SENATOR FROM TEXAS

Senator CRUZ. Thank you, Mr. Chairman. Welcome to the witnesses.

Mr. Enright, I want to go back to the topic that a couple other Senators raised with you, which is China. After a cyber attack comprised the Gmail accounts of dozens of Chinese human rights advocates, Google decided in March of 2010 to shut down its operations in China.

At the time, Google released a statement that said, "We want as many people in the world as possible to have access to our services, including users in Mainland China. Yet the Chinese Government has been crystal clear throughout our discussions that self-censorship is a non-negotiable legal requirement."

Despite taking this principled stand in 2010, it's been reported last month that Google has been secretly developing a search engine for China as part of a project known as Dragonfly. Are those reports accurate?

Mr. ENRIGHT. Senator, thank you for the question. As we've said, I'm aware of those reports. I need to be clear for the record that my understanding is that we are not close to launching a search product in China and whether we eventually could or would remains unclear.

Senator CRUZ. Is there a Project Dragonfly and, if there is, what is it?

Mr. ENRIGHT. We have an array of internal projects and I wouldn't think that it was necessarily appropriate for a privacy conversation to speculate as to what we might be looking at in terms of a product launch in some part of the world.

Senator CRUZ. So you're not answering my question then on Project Dragonfly?

Mr. ENRIGHT. There is a Project Dragonfly.

Senator CRUZ. And it's focused on a search engine in China, is that accurate?

Mr. ENRIGHT. There is no—we are not close to launching a search product——

Senator CRUZ. You're saying you're not close to launching. I'm asking is the topic of Project Dragonfly, is it a project to develop a search engine in China? I didn't ask timing of launch. I asked what it is.

Mr. ENRIGHT. Understood. I am not clear on the contours of what is in scope or out of scope for that project, but I can say is if we were close to a launching a search product in China, myself and my team would be very actively engaged to ensure that it was going through the appropriate privacy review process and that it was consistent with our privacy values and the commitments that we've made to our users.

Senator CRUZ. In your opinion, does China engage in censoring its citizens?

Mr. ENRIGHT. As the privacy representative for Google, I'm not sure that I have an informed opinion on that question.

Senator CRUZ. It has also been reported that more than 3,100 Google employees sent a letter to Google's CEO earlier this year protesting the company's work on Project Maven, a Pentagon pilot program aimed at speeding up the Defense Department's use of artificial intelligence technologies.

Likewise, 1,400 Google employees signed a letter last month protesting Google's plans to create a censored search engine for China.

Mr. Enright, you've worked for Google since 2011. Does it concern you that more than twice as many employees at Google have protested working with the U.S. military than have protested creating a censored search engine for China?

Mr. ENRIGHT. Senator, I take a great deal of pride in the fact that Google is an organization that allows employees to voice their opinions, including opinions about product strategy, product decisions, right up to the senior-most leadership of the organization.

As to Project Maven, again, my understanding is that there was internal concern raised. Employees were given a voice. There was

a significant internal discussion around the project. It ultimately affected the strategic direction of leadership and while Google continues to commit to meeting the responsibilities of our initial Maven contract and we continue to work with the United States Government, the Department of Defense in certain areas, including cyber security, health care, and productivity, but we are focusing on making sure that our collaborations with the Government are consistent with our core values.

Senator CRUZ. Let me try again because your answer didn't answer my question.

Does it concern you that more than twice as many Google employees expressed concern about working with the U.S. military as did concern about being complicit in China censoring its citizens?

Mr. ENRIGHT. It encourages me that Google is a place where employees are able to voice those kinds of concerns about projects that they want to ensure are consistent with our values.

Senator CRUZ. Do Google search results as a systemic matter tend to favor one political party over another?

Mr. ENRIGHT. No, sir. We build products for everyone and in my experience, I see no evidence of bias in the way that our products and services operate.

Senator CRUZ. OK. So you gave a categorical answer no, they don't favor one party over the other. What is the basis for that answer? Upon what data do you rely?

Mr. ENRIGHT. The basis for that answer, Senator, is my own experience and my own understanding of our products. I have not reviewed data, so.

Senator CRUZ. Does Google assess whether its search results are biased in favor of one political party or another?

Mr. ENRIGHT. My understanding, again as a privacy executive at Google, so we're stepping outside of my core domain here, but my understanding is that one of the paramount design decisions for our engineering teams in our many products is that we are designing for everyone——

Senator CRUZ. Mr. Enright, we're having a problem with answering the question. I asked if Google assesses this question, if you've studied it.

I can tell you millions of Americans, I can tell you millions of Texans believe that big tech companies are actively censoring the speech of American citizens and are silencing the voices of conservatives.

One of the frustrating things about this issue is there's almost no transparency. There are almost no public data to assess if that's accurate or not.

So my question is, is Google analyzing the question? Is Google actually looking—not your own personal experiences searching, but are you assessing it empirically? Upon what data do you make testimony in this committee that Google is not favoring in its search results one party over another or one candidate over another?

Mr. ENRIGHT. As the Chief Privacy Officer of Google, this is not within my core domain. So I can only speak to my own experience and the things that are my responsibilities within the organization, but within my purview, I have never seen any evidence of bias and I consistently see a commitment.

Senator CRUZ. OK. I'm going to try just one more time. Are you aware of any efforts of Google to assess whether search results have a political bias? Don't give me a statement they don't have a bias. Are you aware of efforts to actually empirically assess and determine it?

Mr. ENRIGHT. As Chief Privacy Officer of Google, I am not aware of such efforts.

Senator CRUZ. Thank you.

The CHAIRMAN. Thank you, Senator Cruz.

Well, I think that kind of wraps up our hearing. I'm going to ask unanimous consent to include in the record letters from the Association of National Advertisers, the Interactive Advertising Bureau, the Internet Association, the National Association of federally Insured Credit Unions, Privacy for Cars, and the U.S. Chamber of Commerce. Without objection.

[The letters referred to follow:]

ASSOCIATION OF NATIONAL ADVERTISERS
September 24, 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 Association of National Advertisers ("ANA")[1] commends you for convening the upcoming hearing entitled, "Examining Safeguards for Consumer Data Privacy," and for the Committee on Commerce, Science, and Transportation's ("Commerce Committee" or "Committee") continued work on the important issue of data privacy.

The Commerce Committee has been a leader on data privacy issues since the advent of the modem Internet and we urge the Committee to maintain its careful and thoughtful approach to data policy issues. Dialogue with all stakeholders in the digital economy will be essential to the Committee's ongoing oversight efforts to ensure consumers continue to benefit from an open, competitive, and im1ovative digital marketplace. To that end, as you consider data privacy issues, it is central to consider the myriad benefits of data and advertising, which fuel economic growth, foster a wide array of affordable media choices that educates the public, and drive im1ovation and consumer value.

In today's digital economy, data and advertising have become essential in the provision of innovative products and services to consumers, and information about such products and services.[2] Data improves advertising, which in turn creates for consumers a vibrant ad-supported ecosystem delivering essential products, services, and media content. Data also is vitally important to U.S. economic competitiveness. Ideas developed in the United States by statisticians and econometricians, running

[1] The ANA makes a difference for individuals, brands, and the industry by driving growth, advancing the interests of marketers and promoting and protecting the well-being of the marketing community. Founded in 191O, the ANA provides leadership that advances marketing excellence and shapes the future of the industry. The ANA's membership includes nearly 2,000 companies with 25,000 brands that engage almost 150,000 industry professionals and collectively spend or support more than $400 billion in marketing and advertising annually. The membership is comprised of more than I, I00 client-side marketers and more than 800 marketing service provider members, which include leading marketing data science and technology suppliers, ad agencies, law firms, consultants, and vendors. Further enriching the ecosystem is the work of the nonprofit ANA Educational Foundation, which has the mission of enhancing the understanding of advertising and marketing within the academic and marketing communities.

[2] In a recent Zogby survey, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content. Zogby Analytics, *Public Opinion Survey on Value of the Ad-Supported Internet* (May 2016). The Zogby survey also found that consumers value the ad-supported content and services at almost $1,200 a year. Digital Advertising Alliance, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth $1,200/Year; 85 percent Prefer Ad-Supported Internet to Paid,* PR Newswire (May 11, 2016).

on U.S.-designed hardware, and coded in algorithms developed and tested in the research offices of U.S. firms, are used to generate significant revenues throughout the world. A study led by Prof. John Deighton at the Harvard Business School reported that the ad-supported Internet ecosystem generated $1.121 trillion for the U.S. economy and was responsible for 10.4 million jobs in the U.S. in 2016.[3]

Increasingly, however, the digital economy faces ill-conceived requirements regulating the collection and use of data, including some adopted at the state and international levels, such as the hastily enacted California Consumer Privacy Act ("CCPA") and the European Union's General Data Protection Regulation ("GDPR").[4] These rules limit legitimate and consumer valued uses of data, overburden consumers with notices, allow for broad access to consumer data without thoughtful safeguards to protect against fraud and criminal behavior, and negatively impact the efficiency and effectiveness of the digital economy. Stakeholders across the spectrum are raising alanns with respect to the defective provisions of the CCPA.[5] In particular, the CCPA's statutory damages and private right of action related to data breaches have the potential to bankrupt a broad range of companies even if the data released causes no consumer harm. Similar problems have emerged with GDPR, which imposes literally hundreds of rules on the collection and use of data. We have already seen a number of companies pull their products and services out of Europe due to the significant resources required to comply with the GDPR's prescriptive and voluminous rules.[6]

The first results of the CCPA and GDPR experiments are in, and the evidence is showing that these laws are harmful to consumers and businesses, and will have a chilling effect on innovation. The rules also are overlapping and inconsistent, which is creating a balkanized patchwork of regulations that consumers will not understand, that impose significant costs on businesses, and that serve as a major barrier to entry. As such, to fully understand the CCPA's and GDPR's negative effects on consumers and competition, and to inform its continued oversight efforts, we recommend that the Committee instruct the Department of Commerce and the Federal Trade Commission to carry out a detailed review of the impacts of GDPR and CCPA. Such a review will be crucial in evaluating the various approaches to privacy and data security that have already been imposed and are presently being proposed across the country. The review also will help inform policy decisions on a new Federal privacy framework that neither jeopardizes the United States' competitive advantage in technology and innovation nor strips consumers of the benefit and enjoyment of a data-driven Internet ecosystem.

To help ensure that consumers continue to enjoy the online content, products, and services they value and expect, the data that underpins advertising and marketing must continue to be available. The Congress can and should act to prevent and preempt unacceptable outcomes for U.S. consumers and the economy while at the same time considering a new privacy paradigm that includes strong consumer privacy protections and that maintains the United States' leadership in the digital economy.

The ANA appreciates the opportunity to comment on this hearing and we ask that this letter be placed in the hearing record. Please contact Dan Jaffe, Group Executive Vice President, at *djaffe@ana.net* or (202) 296–2359 with any questions. We look forward to working with the Committee on these important matters.

Respectfully submitted,

DAN JAFFE,
Group EVP Government Relations,
Association of National Advertisers.

---

[3] John Deighton, Leora Kornfeld, Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem,* IAB (2017).

[4] Cal. Civ. Code § 1798.100 (effective Jan. 1, 2020); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] Dan Jaffe, *Fixing the California Privacy Law Will Require a Serious, Long Term Effort,* ANA (Sept. 4, 2018); Sarah Boot, *No Time to Waste on Fixing Consumer Privacy Law,* CalChamber (Aug. 20, 2018).

[6] Hannah Kuchler, *US small businesses drop EU customers over new data rule,* Financial Times (May 24, 2018).

September 24, 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.

Dear Chairman Thune and Ranking Member Nelson:

The Interactive Advertising Bureau ("IAB") commends the Committee on Commerce, Science, and Transportation ("Committee") for convening its hearing on *Examining Safeguards for Consumer Data Privacy,* and for its continued leadership on this important issue. We are eager to partner with Congress as it looks at the online privacy landscape and considers enhancements to benefit consumers and ensure the U.S. maintains its position as the global data leader.

IAB is comprised of more than 650 member companies, which account for the vast majority of online advertising sold in the United States. Our members' innovative services and technological leadership are the drivers behind the $1.12 trillion advertising-supported U.S. Internet economy, and are responsible for more than 10 million jobs across every state.[1] According to recent research, Americans value their free Internet experience at over $1,200 per year, and 85 percent of consumers indicate that they prefer the existing ad-supported Internet model over more expensive alternatives.[2]

The ad-supported Internet generates tremendous value for consumers, the economy, and the democratization of information. The bedrock for this ecosystem is the responsible collection and use of data, enabling Americans, and the world, to access the content and services they love for little or no cost. Disruption to the advertising-supported Internet could result in a costly, frustrating, and less valuable consumer experience. Any changes to this construct need to be considered with great care.

As the Committee examines the topic of data privacy, IAB offers the following points:

- *Collection and use of data comes with great responsibility, which IAB member companies realize and safeguard.*
  - IAB member companies have moved swiftly to create safeguards to foster privacy and innovation alongside evolving consumer preferences and technology. Our programs have proven and effective results, and could serve as a model for a Federal legislative standard.
  - For example, in 2008, the Digital Advertising Alliance ("DAA") was established to provide consumers with control and enhanced transparency into digital ads. It resulted in the development of the ubiquitous AdChoices Icon that appears more than one trillion times per month.[3] With this tool, consumers have immediate access to relevant information and control over how information is used for advertising.
  - Since its inception, the DAA icon has evolved to keep pace with consumer demand. The program now offers consumers control within apps, across devices, and in Spanish.
  - Recently, the icon was adapted for political ads, providing a new form of transparency and accountability into the funding and identity behind "express advocacy" ads.[4]
  - Similar industry efforts have been successfully developed to prevent fraud and malware from infecting the Internet economy, and ad formats from slowing or hindering consumers' Internet experiences.[5]

---

[1] John Deighton, PhD., *Economic Value of the Advertising-Supported Internet Ecosystem (March 15, 2017) https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017–FINAL2.pdf*

[2] Digital Advertising Alliance, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth $1200/Year, 85 Percent Prefer Ad-Supported Internet to Paid (May 11, 2016) https://digitaladvertisingalliance.org/press-release/zogby-poll*

[3] Digital Advertising Alliance, *https://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-launches-new-industry-focused-website*

[4] Digital Advertising Alliance, *Application of the Self-Regulatory Principles of Transparency & Accountability to Political Advertising (May 2018). https://aboutpoliticalads.org/principles*

[5] The Trustworthy Accountability Group was created to focus on eliminating fraudulent digital advertising traffic, combating malware, fighting ad-supported Internet piracy to promote brand

Continued

- *The exponential growth and innovation in the digital advertising industry over the last decade has been revolutionary for consumers. Any approach to privacy must be flexible and nimble so that "rules of the road" can evolve with innovation and consumer expectations.*
  - As beneficiaries of the economic boom that has been born from online advertising, we acknowledge our role as stewards of consumer data, and the importance of trust to the value exchange with consumers.
  - Consumer awareness about online data collection and usage has steadily grown, due in large part to industry accountability and education programs.
  - However, additional work must be done to promote consumer trust and safety. We believe the time is now to consider sensible legislation to address these pressing challenges.
- *Legislative and regulatory models should provide meaningful consumer controls that are technologically neutral, proportionate to consumer risk, and encourage industry best practices.*
- IAB is concerned that laws such as the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") will result in a patchwork of varying state laws and consumer confusion, and would negatively impact the online user experience.
- Despite the best intentions of those efforts, unintended consequences have resulted in leading American websites going dark in Europe due to the uncertainty around the GDPR's provisions, and the CCPA could lead to an Internet experience in California that contrasts with that of every other state.[6]

While industry efforts have provided effective consumer tools that have been lauded by the Federal Trade Commission, the Department of Commerce, and the White House, there is much more work to be done, and IAB is eager to partner with all stakeholders towards providing greater transparency and control for consumers.[7]

A uniform Federal privacy standard could provide clarity, market certainty, and add fuel to future innovation, while preserving the value and benefit that online advertising brings to the Internet ecosystem.

We would welcome a dialogue around a Federal standard that could strengthen and enhance these programs even further. We are ready to work with the Committee on ideas to enhance consumer privacy while preserving the tremendous value and benefits of the advertising-supported internet.

Sincerely,

DAVID F. GRIMALDI,
Executive Vice President, Public Policy,
Interactive Advertising Bureau.

INTERNET ASSOCIATION
Washington, DC, September 25, 2018

Chairman JOHN THUNE and Ranking Member BILL NELSON,
Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

Thank you for holding today's hearing to examine safeguards for consumer data privacy.

Internet Association [1] (IA) welcomes the opportunity to submit this letter and our enclosed principles for a national privacy framework for the record as part of the

---

integrity, and promoting brand safety through greater transparency. *https://www.tagtoday.net/aboutus/;* The Coalition for Better Ads was created to improve consumers' experience with online advertising through developing and implementing new global standards. *https://www.betterads.org/about/*

[6] Jeff South, Nieman Lab, *More than 1,000 U.S. news sites are still unavailable in Europe, two months after the GDPR took effect (August 7, 2018) http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-stillunavailable-in-europe-two-months-after-gdpr-took-effect*

[7] Digital Advertising Alliance, *White House, DOC, and FTC Commend DAA's Self-Regulatory Program to Protect Consumer Online Privacy (February 23, 2012) https://digitaladvertisingalliance.org/press-release/white-house-doc-and-ftc-commend-daa%E2%80%99s-self-regulatory-program-protect-consumer-online*

[1] Internet Association represents *https://internetassociation.org/our-members/*.

committee's September 26 hearing *"Examining Safeguards for Consumer Data Privacy"*.

IA is the only trade association that exclusively represents leading global Internet companies on matters of public policy. Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the Internet creates unprecedented benefits for society and the economy and, as the voice of the world's leading Internet companies, IA works to ensure legislators, consumers, and other stakeholders understand these benefits.

We urge Congress to pass a Federal privacy law that protects personal data and provides people with more control over how the data they share is seen, used, and handled on and offline. IA released privacy principles in support of an American approach to Federal privacy legislation that is consistent nationwide, proportional, flexible, and enables companies to act as good stewards of personal information provided to them by individuals. IA's proposed principles include:

- *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.
- *Controls.* Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, unless that information is legally required, or is necessary for the basic operation of the business.
- *Access.* Individuals should have reasonable access to the personal information they provide to companies. Personal information may be processed, aggregated, and analyzed to enable companies to provide services to individuals.
- *Correction.* Individuals should have the ability to correct the personal information they provide to companies, except where companies have a legitimate need or legal obligation to maintain it.
- *Deletion.* Individuals should have the ability to request the deletion of the personal information they provide to companies when it's no longer necessary to provide services, except where companies have a legitimate need or legal obligation to maintain it.
- *Portability.* Individuals should have the ability to take the personal information they have provided to one company and provide it to another company that provides a similar service.

Internet Association's privacy principles place a heavy emphasis on context as the basis for any new national privacy framework. This means that such a framework must be flexible, taking into account the reasonable expectations individuals have regarding how the personal information they provide companies will be used and shared, the sensitivity of personal information they provide to companies, and the concrete risk to individuals of the potential misuse or unanticipated sharing of such personal information. This risk-based approach will protect consumers when they need it most and also recognize that data—even the same piece of information—can present different harms based on who has it and how it is being used.

We also believe that any new national consumer privacy framework must be both technology-neutral and sector-neutral, applying to both online and offline companies; and must be mindful of the impact of new requirements on small and medium sized companies.

We reiterate our support for the committee's efforts to address this important issue, and we are committed to working with you, consumers, and other stakeholders to develop solutions that enhance consumer privacy as well as promote economic growth and innovation.

Sincerely,

MICHAEL BECKERMAN,
President and CEO.

CC:

Introduction

The time is right to modernize our Federal rules and develop a national framework for consumer privacy. That framework should be consistent nationwide, proportional, flexible, and should encourage companies to act as good stewards of the personal information provided to them by individuals.

As policymakers and stakeholders work on an updated approach to privacy, we must ensure that a national privacy framework:

- Protects individuals' personal information and fosters trust by enabling individuals to understand their rights regarding how their personal information is collected, used, and shared;
- Meets individuals' reasonable expectations with respect to how the personal information they provide companies is collected, used, and shared, and the context-dependant choices they have;
- Promotes innovation and economic growth, enabling online services to create jobs and support our economy;
- Demonstrates U.S. leadership in innovation and tech policy globally;
- Is mindful of the impact of regulation on small-and medium-sized companies; and
- Applies consistently across all entities to the extent they are not already regulated at the Federal level.

Context for principles: Our country's vibrant Internet ecosystem provides individuals with unprecedented personal, social, professional, educational, and financial benefits, contributing an estimated 6 percent of U.S. GDP and nearly 3 million American jobs. The Internet enables all levels of government and every sector of the economy to become more citizen-and consumer-centric by providing innovative tools, services, and information, and allowing for a more efficient use of resources.

IA companies believe trust is fundamental to their relationship with individuals. Our member companies know that to be successful they must meet individuals' reasonable expectations with respect to how the personal information they provide to companies will be collected, used, and shared. That is why our member companies are committed to transparent data practices, and to continually refining their consumer-facing policies so that they are clear, accurate, and easily understood by ordinary individuals. Additionally, our member companies have developed numerous tools and features to make it easy for individuals to manage the personal information they share, as well as their online experiences.

There are a range of strong privacy, data security, consumer protection, and anti-discrimination laws that exist today. These include Section 5 of the FTC Act and the Clayton Act, as well as more than 15 other Federal statutes and implementing regulations that are sector specific or relate to particular activities.[2] Additionally, there are myriad state laws relating to privacy and data security, enforced by state attorneys general or private litigants, including state data breach notification statutes and unfair and deceptive acts and practices statutes; data security and encryption laws; and a variety of other privacy laws that relate to online privacy, social security numbers, and data brokers. Our member companies comply with these current laws as well as with self-regulatory principles and rules that govern how they operate and do business.[3] However, this array of laws also creates a "patchwork" effect that complicate compliance efforts and lead to inconsistent experiences for individuals. A new, comprehensive national framework would create more consistent privacy protections that bolster consumers' privacy and ease compliance for companies.

This document sets forth: (1) principles for a national privacy framework, and (2) considerations for policymakers when evaluating such a national privacy framework.

Privacy Principles

These privacy principles aim to protect an individual's personal information, which we define as any information capable of identifying a specific individual or a device that belongs to that individual.

---

[2] These are the Children's Online Privacy Protection Act ("COPPA") and the FTC's COPPA Rule; the Gramm-Leach-Bliley Act, and the FTC's Privacy and Safeguards Rules; the Electronic Fund Transfer Act; the Fair Credit Reporting Act; the Fair and Accurate Credit Transactions Act; the Equal Credit Opportunity Act; The Truth in Lending Act; the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN–SPAM") Act of 2003 and the FTC's CAN–SPAN Rule; the Telephone Consumer Protection Act; the Restore Online Shopper's Confidence Act; the Video Privacy Protection Act; the Cable Act; the Electronic Communications Privacy Act; the Computer Fraud and Abuse Act; the Stored Communications Act; the Telemarketing and Consumer Fraud and Abuse Prevention Act and the FTC's Telemarketing Sales Rule, including the Do Not Call Rule and Registry; and the U.S. Safe Web Act.

[3] These self-regulatory bodies have developed their own codes of conduct, including the *Data and Marketing Associations Ethical Business Practices;* the *Network Advertising Initiative's 2018 Code of Conduct;* the *Digital Advertising Alliance's set of Self-Regulatory Principles* relating to online advertising, which are enforced by the *Accountability Program of the Council of Better Business Bureaus;* and the Payment Security Industry Data Security Standards (PCI–DSS), for those that accept payment cards.

- *Transparency.* A national privacy framework should give individuals the ability to know whether and how personal information they provide to companies is used and shared with other entities, and if personal information is shared, the categories of entities with whom it is shared, and the purposes for which it is shared.
- *Controls.* Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, except where that information is necessary for the basic operation of the business or when doing so could lead to a violation of the law.
- *Access.* Individuals should have reasonable access to the personal information they provide to companies. Personal information may be processed, aggregated, and analysed to enable companies to provide services to individuals. Safeguards should be included to ensure that giving an individual the ability to access their personal information does not unreasonably interfere with other individuals' privacy, safety, or security, or a company's business operations.
- *Correction.* Individuals should have the ability to correct the personal information they provide to companies, except where companies have a legitimate need or legal obligation to maintain it.
- *Deletion:* Individuals should have the ability to request the deletion of the personal information they provide to companies where that information is no longer necessary to provide the services, except where companies have a legitimate need or legal obligation to maintain it.
- *Portability.* Individuals should have the ability to obtain the personal information they have provided to one company and provide it to another company that provides a similar service for which the information is necessary.

The adoption of the principles identified above would enhance individuals' personal privacy and ensure individuals' trust. To ensure the effectiveness of a national privacy framework, these principles must be balanced against: (1) competing individual rights, including freedom of speech and expression; (2) other parties' privacy interests; (3) data security interests; (4) companies' needs to protect against fraud or other unlawful activity, or individual safety; (5) companies' requirements to comply with valid law enforcement requests or judicial proceedings; (6) whether the exercise of the rights afforded individuals are unduly burdensome or excessive in specific instances; and (7) whether individuals' exercise of their rights would require companies to collect or process additional personal information about that individual.

Proposed Considerations for Policymakers

Fostering privacy and security innovation. A national framework should not prevent companies from designing and implementing internal systems and procedures that enhance the privacy of each individual's personal information. Companies should take into account privacy and data security when they design and update their services, for example, by de-identifying, pseudonymizing, or aggregating data.

A national data breach notification law. A national framework should specifically preempt the patchwork of different data breach notification laws in all 50 states and the District of Columbia to provide consistency for individuals and companies alike. This national standard should protect individuals and their personal information through clear notifications, define a harm-based trigger for notification to avoid notice fatigue, and allow companies flexibility in how they notify individuals of unauthorized access to their personal information.

Technology and sector neutrality. A national privacy framework should include protections that are consistent for individuals across products and services. Such a framework should be both technology neutral (no specific technology mandates) and sector neutral (applying to online and offline companies alike).

Performance standard based approach. A national privacy framework should focus on accomplishing privacy and data security protections, but laws and regulations should avoid a prescriptive approach to doing so, as such an approach may not be appropriate for all companies and may well become obsolete in light of rapidly developing technology.

Risk-based framework. A national privacy framework should be grounded in a risk-based approach, based on the sensitivity of the personal information, the context of its collection and use, and the risk of tangible harm for its misuse or unauthorized access. Consistent with FTC data security order provisions and the FTC's unfairness standard, companies should identify and address reasonably foreseeable risks to the privacy and the security of personal information where the result of failing to address the risk would cause, or be likely to cause, tangible consumer harm.

A modern and consistent national framework for individuals and companies. A national privacy framework should be consistent throughout all states, preempting state consumer privacy and data security laws. A strong national baseline creates clear rules for companies and ensures that individuals across the United States can expect consistent data protections from companies that hold their personal information. A national privacy framework should primarily be enforced by the FTC at the Federal level and by state attorneys general at the state level, where the FTC declines to act.

NATIONAL ASSOCIATION OF FEDERALLY-INSURED CREDIT UNIONS
Arlington, VA, September 25, 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: Tomorrow's Hearing, "Examining Safeguards for Consumer Data Privacy"

Dear Chairman Thune and Ranking Member Nelson:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only trade association exclusively representing the Federal interests of our Nation's federally-insured credit unions, I write today in conjunction with tomorrow's hearing, "Examining Safeguards for Consumer Data Privacy." We appreciate the Committee's continued focus on protecting consumer information and data.

While tomorrow's hearing focuses on privacy of consumer data, we urge the Committee to not lose focus on the need for data protection, particularly when it comes to establishing a national standard of consumer data security. As NAFCU has previously communicated to the Committee, there is a need for a national data security standard for entities that collect and store consumers' personal and financial information that are not already subject to the same stringent requirements that depository institutions are under the *Gramm-Leach-Bliley Act* (GLBA).

Unfortunately, data breaches have become a constant concern of the American people. Major data breaches now occur with an unacceptable level of regularity. Polling has found that two-thirds of U.S. adults are frequently or occasionally concerned about having their credit card information stolen by hackers. These staggering survey results speak for themselves and should demonstrate the need for greater national attention to this issue.

Credit unions suffer steep losses in re-establishing member safety after a data breach occurs and are often forced to absorb fraud-related losses in its wake. Credit union members often turn to their credit union for answers and support when data breaches occur. As credit unions are not-for-profit cooperatives, credit union members are the ones that are ultimately impacted by these costs. Negligent entities should be held financially liable for any losses that occurred due to breaches on their end so that consumers are not left holding the bag.

As the Committee examines the larger consumer data privacy debate, we urge you to recognize that the security of consumer data is another important reason why a national data security standard needs to be considered. On behalf of our Nation's credit unions and their more than 114 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information please contact me or Allyson Browning, NAFCU's Associate Director of Legislative Affairs, at 703–842–2836 or abrowning@nafcu.org.

Sincerely,

BRAD THALER
Vice President of Legislative Affairs.

cc: Members of the Senate Committee on Commerce, Science, & Transportation

PREPARED STATEMENT FROM PRIVACY4CARS

Good morning, Chairman Thune, Ranking Member Nelson, and distinguished members of the U.S. Senate Committee on Commerce, Science, and Transportation. Privacy4Cars is pleased to present these comments to the Committee concerning today's hearing to "Examine Safeguards for Consumer Data Privacy" and we respectfully request that this statement be made a part of the official record of this hearing.

Consumers here at home and abroad are demanding to know how and where their personal information is being gathered and stored. This Committee has been diligent in focusing on the protection, transparency, and use of consumers' personal data and we commend the Committee for holding this public hearing.

Privacy4Cars [1] was founded by a vehicle privacy and cybersecurity expert and is dedicated to providing simple and pragmatic privacy solutions to both consumers and businesses in the automotive industry. We have first-hand experience in the industry and we work with many industry players who are frustrated with how modern vehicles retain Personally Identifiable Information (PII) in their In-Vehicle Infotainment Systems (IVIS), and the complexity required to remove all information properly.

We launched Privacy4Cars and developed the first and only currently-accessible mobile process designed to erase PII from modern vehicles. To fulfill our social mission, we decided that our namesake Privacy4Cars app should be available as a free download for consumers on iOS and Android devices, so they would have a tool to protect themselves against potential security breaches and theft of data, which often includes phone numbers, call logs, location history, favorite destinations—including home addresses—and even garage door codes.

According to a recent internal poll among IARA members published in the spring of 2019, 79 percent of the respondents—all experts in the used vehicle industry—are concerned about the PII captured by modern IVIS. The reason for concern is that multiple studies conducted by IARA or Privacy4Cars demonstrated the percentage of vehicles still retaining their users' PII at the time of resale is staggering. In the summer of 2017 IARA analyzed a random sample of 394 vehicles at auto auctions. The sample size represented 32 models and makes manufactured between 1995 and 2017. In the sample tested, most vehicles being resold still contained personal data of the previous vehicles' users in the navigation and/or Bluetooth module.

A second study was performed by Privacy4Cars with over 600 vehicles belonging to rental car fleets. This subsequent testing showed that nearly 99 percent of the vehicles being rented or resold contained personal information of the renters. Privacy4Cars performed a third test of 96 vehicles manufactured between 2001 and 2018 at an auto auction in the United Kingdom and the results were equally alarming. 86 percent of the randomly-selected vehicles tested still retained PII in the IVIS.

Privacy4Cars strongly believes the evidence collected through its studies suggests that there has not been an adequate effort to educate vehicle users on the dangers of leaving their Personally Identifiable Information in vehicles they no longer use. It is ludicrous to imagine individuals being willing to hand their cell phones—with all their personal data—over to strangers. Yet the driving public often fail to realize that they are essentially doing the same thing every time they sell a vehicle, return a rental car, or participate in a car sharing or subscription program.

One simple way that vehicle owners and operators can protect their privacy is to be mindful of the data stored in vehicle infotainment systems and properly erase the information—especially if the car is sold, leased, rented, or shared. Unfortunately, to date, the industry has not prioritized designing IVIS systems that can simply and reliably prevent theft and abuse of personal information stored in vehicles.

Neither has the industry adopted the practice of employing "safety nets" by removing vehicle-stored PII such as navigation data, phone data, and garage codes before a vehicle is sold, resold or traded. While the automotive industry and NHTSA have issued recommendations and standards for Event Data Recorders (*https://*

[1] Our founder, Mr. Andrea Amico, has been heading the Privacy and Cybersecurity initiative at the International Automotive Remarketing Alliance (IARA, *www.iara.biz*), the industry association that reunites many of the leading players in the $100 billion vehicle wholesaling industry in the U.S. and Canada, including automotive OEMs, automotive finance companies as large as captives and national blue-chip banks to smaller regional auto leasing and lending companies, most of the main auto auctions, large fleet management and fleet companies such as rentals, vehicle repossession companies, dealers, and many other service providers. At IARA, Amico spearheaded the formation of a partnership with Auto-ISAC, the Information Sharing and Analysis Center, established by the automotive industry to address cybersecurity and privacy issues.

www.nhtsa.gov/research-data/event-data-recorder#overview-10516), In-Vehicle Infotainment Systems do not fall under that framework. Most IVIS also fail to include some of the basic data protection techniques that are commonplace with modern computing and mobile devices, such as authentication and encryption.

As the industry continues to deploy vehicles that are capturing larger amounts of data and are increasingly becoming "connected," Privacy4Cars believes the risks and the importance of protecting vehicle users' PII will dramatically increase. In 2014 the Alliance of Automotive Manufacturers committed to a set of Consumer Privacy Protection Principles (*https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf*).

We encourage all players in the automotive ecosystem—including companies that could potentially access any data collected or transmitted by vehicles—to commit to the same principles of Transparency, Choice, Respect for Context, Data Minimization, De-Identification, Retention, and Data Security.

As modern-day vehicles increasingly resemble smartphones, we urge the Committee to draw parallels between the rules and regulations adopted in that context and apply those common-sense protections to vehicles, including cybersecurity-by-design and privacy-by-design best practices. We also encourage the Committee to clarify a single regulatory owner for privacy issues with vehicles, an approach similar to the role NHTSA has prescribed for vehicle safety.

Thank you for the opportunity to provide these comments. Privacy4Cars looks forward to working with all stakeholders to address the challenges of consumer proprietary information in this exciting era of connected and autonomous vehicles. We welcome the opportunity to be a resource for this Committee in the areas of industry data, insights, or expertise.

Respectfully submitted,

ANDREA AMICO,
Privacy4Cars.

September 26, 2018

The Honorable John Thune
Chairman
Committee on Commerce, Science
& Transportation
Washington, DC 20510

The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science
& Transportation
Washington, DC 20510

Dear Chairman Thune and Ranking Member Nelson,

We, the undersigned organizations and trade associations, thank you for holding today's hearing examining safeguards for consumer data privacy. In today's digital economy, we believe that it is vital consumers know that data is used responsibly and that their privacy is protected.

We urge Congress to pass a federal privacy law that will put an end to consumer confusion, respect privacy, and provide regulatory certainty to the business community.

As the Committee continues to address this important issue, we stand ready to work with you to develop solutions to enhance consumer privacy as well as promote economic growth and innovation.

Sincerely,

American Hotel & Lodging Association
CTIA-Everything Wireless
CompTIA
Internet Association
National Association of Manufacturers
National Retail Federation
NCTA-The Internet and Broadband Association
Software & Information Industry Association
U.S. Chamber of Commerce
U.S. Telecom-The Broadband Association
U.S. Travel Association

The CHAIRMAN. We will keep the hearing record open for a couple of weeks and ask Senators who have questions that they want to submit for the record to get those in and then as you receive those, if you could as quickly as possible submit your written answers but no later than October 24, Wednesday.

We'll continue to pursue this issue and, as I mentioned, this will be the first of what I suspect will be other efforts to get input from those who are affected by the privacy issue and have an interest in seeing Congress move forward in a way that is consistent with what we think are many of the principles that you have outlined today but certainly giving consumers the choices and opportunities to meaningfully consent, make sure there's transparency in the policies that you all employ, knowing full well that there are other models out there in Europe and California, and much of the testimony today obviously dealt with the need to have a consistent uniform policy that can be applied to everyone across the board and interesting to hear the comments with respect to tech companies and ISPs today, as well.

So we appreciate your testimony, your responses to our questions. I think it has been very informative and it will help shape what we do going forward. I think there were a lot of important questions asked today and some answers I think will, as I said, be very helpful in our deliberations moving forward.

So thank you all for being here, for your willingness to testify, and we'll look forward to continuing to have this conversation, and I'm certain it won't be the first but probably one of many conversations going forward.

With that, this hearing is adjourned.

[Whereupon, at 12:30 p.m., the hearing was adjourned.]

A P P E N D I X

September 19, 2018

Chairman JOHN THUNE,
Ranking Member BILL NELSON,
Senate Commerce Committee,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson,

On behalf of leading consumer privacy organizations in the United States, we write to express surprise and concern that not a single consumer representative was invited to testify at the September 26 hearing "Examining Safeguards for Consumer Data Privacy." While we appreciate your consideration of these important issues, we do not understand why the Committee has chosen to exclude the voice of consumers.

First, by tradition both the Senate and House Commerce Committees routinely invite consumers to testify at hearings concerning consumer interests. The hearing next week on consumer privacy, which includes six industry witnesses, may be one of the first ever convened when not a single consumer group was asked to testify.

Second, the absence of consumer representatives all but ensures a narrow discussion, focused on policy alternatives favored by business groups. Will any of your witnesses recommend Federal baseline legislation, heightened penalties for data breaches, the end of arbitration clauses, the establishment of a privacy agency in the U.S., techniques for data minimization, or algorithmic transparency to prevent the secret profiling of American consumers? These are all safeguards favored by many consumer privacy organizations that should be considered by Committee Members. How can members of the Committee develop sensible solutions if they are not even aware of the full range of options?

Third, the United States Senate is first and foremost a public institution, accountable to the people. While we have no objection to the participation of business groups in Senate hearings on consumer privacy, the Senate's first instinct should be to hear from the American public on these important issues. Are you aware, for example, that identity theft is among the top concerns of American consumers? Do you know that the recent Harris survey found that 78 percent of U.S. respondents say a company's ability to keep their data private is "extremely important," but only 20 percent "completely trust" organizations they interact with to maintain the privacy of their data?

We urge you to invite consumer witnesses to the September 26 hearing. If that is not possible at this time, we ask that you announce a date certain for a hearing in the Senate Commerce Committee at which consumer privacy organizations will be given the opportunity to speak with you about this important issue.

Thank you for your consideration of our views.

Sincerely,

Access Humboldt
American Civil Liberties Union
American Policy Center
Campaign for Commercial Free Childhood
Center for Digital Democracy
Center for Democracy & Technology
Center for Media Justice
Common Cause
Common Sense Kids Action
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Customer Commons
Defending Rights & Dissent
Digital Privacy Alliance
Electronic Frontier Foundation
Electronic Privacy Information Center
The Free Press Action Fund
National Association of Consumer Advocates
National Consumers League
New America's Open Technology Institute
Patient Privacy Rights

Privacy Rights Clearinghouse
Privacy Times
U.S. PIRG
World Privacy Forum

ACCESS NOW
September 19, 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.

Dear Senators,

Thank you for scheduling next week's hearing on "Examining Safeguards for Consumer Data Privacy."[1] We write today to emphasize the importance of Congressional action on data protection in the United States. We are disappointed that the September 26 hearing currently includes only voices from private industry. We strongly urge the Committee to include academics and representatives from civil society with expertise in data protection.

Current Inadequacies in United States Law

In the current digital age, companies have access to substantially more data about individuals than at any time throughout history, a reality becoming aggressively worse with the continued introduction of "internet of things" devices into our daily lives. While many governments around the world have responded by implementing data protection laws, the United States lags behind. The U.S. has instead established a "sectoral" approach to privacy adopted over time. This means that, at a Federal level, we have implemented a patchwork of laws that provide some protections for certain types of data, like data pertaining to students or health information. There is no blanket protection from unchecked data collection, misuse, manipulation, or abuse. In its absence, we have relied on authority given to the Federal Trade Commission ("FTC") to pursue companies that engage in unfair or deceptive trade practices.

This status quo is inadequate at meaningfully protecting users from threats to their data. Take, for example, the circumstances between Cambridge Analytica and Facebook that has received attention as of late.[2] Earlier this year, it was revealed that Cambridge Analytica retained personal information of approximately 87 million (or more) Facebook users that it had received from researcher Aleksandr Kogan through an app he had designed using Facebook's API ("application programming interface"). The app allowed Kogan to access personal information not only about app users but also their Facebook friends, who had not, and in fact could not have, consented to the use of their data. Cambridge Analytica analyzed and used the data to create and purchase highly targeted ads that were used for the 2016 U.S. presidential elections, as well as potentially for other high-profile elections and debates. Company executives have claimed that Cambridge Analytica has been involved in elections around the world, including the U.K., Argentina, India, Mexico, Nigeria, Kenya, and the Czech Republic.

The data at issue in this example did not fall into one of the limited areas where the United States has legislated on privacy. Additionally, at the time that this incident occurred, Facebook was already subject to a consent decree with the FTC which was neither able to prevent it nor did it ensure timely remedy.[3] Notably, one of the standard clauses in FTC consent decrees, including the one with Facebook, is the requirement for an independent audit (or assessment). While these audits may have been able to provide a means for responding to this and similar incidents, experts have flagged their deficiencies:

> *"These audits, as a practical matter, are often the only "tooth" in FTC orders to protect consumer privacy. They are critically important to accomplishing the agency's privacy mission. As such, a failure to attend to their robust enforcement*

---

[1] *https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=240B5C17-CBD5-4039-A9E4-CF2FADFF4712.*

[2] *https://www.accessnow.org/its-not-a-bug-its-a-feature-how-cambridge-analytica-demonstrates-the-desperate-need-for-data-protection/.*

[3] *https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.*

can have unintended consequences, and arguably, provide consumers with a false sense of security."[4]

Data Protection in the United States

Strong Federal data protection legislation is needed to remedy these shortcomings in U.S law. Such a standard not only will respond to increasingly important needs, but it will provide protections for people in the United States on par with those that people enjoy in an ever-growing number of other countries and regions, including the whole of the European Union. A data protection law will also demonstrate that data stored by companies in the United States will adequately protect user information, assisting with ensuring free flows of data across geographic borders. Finally, a law can provide important guidance and clarity for private industry in this important area.

In order to provide meaningful protections for individuals, data protection legislation must combine a series of affirmative rights with affirmative obligations for entities that process data. Appropriate legislation should also include a series of government investments to incentivize research and development into privacy-protective practices and behaviors and helping position the United States as a leader of data protection.[5]

We have identified several provisions that we believe should be a part of any data protection proposal.[6] Some of these provisions include:

- *Individual rights to information, access, rectification, portability, and erasure*—ensuring that people who have their data process have the ability to know what data has been collected, rectify incorrect data, and easily change or leave services
- *Government investment*—incentives for companies who pursue privacy-protective business models and practices, including through grant programs and preferences in bidding for government contracts
- *Building and strengthening Federal agencies*—pursuing the development of an independent data protection commission with authority over implementation of the law as well as ability to conduct investigations and issue sanctions; direction of this new agency or an existing body to conduct research into the short- and long-term consequences of data breaches, including breaches of non-financial information
- *Data breach notification*—a blanket Federal standard to require general public notification of all data breaches, with individualized notification for breaches that could result in potential harm, including emotional harm
- *Corporate obligations for obtaining consent and limiting data collection*—implementing requirements that require specific, enumerated reasons to allow collection of data and ensuring that it is only collected pursuant to meaningful, informed, uncoerced consent

The need for academic and civil society representation

It is important to note that the scheduled hearing is set to include *only* voices from private industry, including major players in the data ecosystem like AT&T, Google, and Amazon. Data protection may provide benefits to private industry in the form of certainty and standardization of international obligations. However, while data protection is inherently a concept that stands to protect the data of individuals, corporate interests do not align with the interests of people on this area. In fact, recently three major trade groups have published "principles" for data protection, with each of them falling short of any set of standards supported by groups who represent individual interests, including the provisions that we describe above.

In order to ensure a comprehensive hearing that provides committee members with important viewpoints and areas of expertise, we highly recommend the addition of advocates, academics, and independent data protection experts. While we believe it is most effective to include these perspectives on the panel alongside the corporate interests to allow for conflicting positions to be aired and ensure equal attention from committee members, a second panel could also be added, at a minimum, to secure an inclusive reflection on the issues.

---

[4] *https://cyberlaw.stanford.edu/blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders.*

[5] Unfortunately, none of the current legislative proposals pending in Congress provides for the necessary levels of user protection. To view our complete analysis of current bills, *see https://www.accessnow.org/cms/assets/uploads/2018/04/USG-Data-Protection-Bills.pdf.*

[6] The full list of our recommendations is available at *https://www.accessnow.org/data-protection-in-the-united-states-where-do-we-go-from-here/.*

Thank you again for your time and attention to this important matter. We appreciate your serious consideration of data protection and are available to provide any additional information or analysis that may be useful to committee members.

About Access Now

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[7] By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. Access Now maintains presences in eleven cities around the world, including in the policy centers of Washington, DC and Brussels.

Sincerely,

AMIE STEPANOVICH,
U.S. Policy Manager.

ELECTRONIC FRONTIER FOUNDATION
San Francisco, CA, September 24, 2018

Hon. JOHN THUNE,
Chairman,
Committee on Commerce, Science, and Transportation,
Washington, DC.

Hon. BILL NELSON,
Ranking Member,
Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 38,000 dues-paying members and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. Furthermore, we work to ensure that the rights and freedoms of individuals are retained and enhanced as their use of technology grows.

EFF submits this letter to the Senate Commerce Committee to detail the dangers to individual user privacy posed by industry suggestions that Congress should wipe the slate clean of state privacy laws through preemption. Many states have already created strong statutory and other protections of user privacy. If Congress enacts data privacy legislation that is weaker than the existing state data privacy laws, and simultaneously preempts the stronger state data privacy laws, the result will be a massive step backwards for user privacy. We urge the Committee to recognize the scope of what is being asked before acting on Federal legislation, as the lives of technology users and their currently existing rights increasingly overlap with their Internet usage, and as data brokers grow increasingly sophisticated at mining and monetizing information about our off-line activity.

In essence, a Federal law that sweeps broadly in its preemption could reduce or outright eliminate privacy protections that Congress has no intent to eliminate, such as laws that protect social security numbers,[1] prohibit deceptive trade practices,[2] and protect the confidentiality of library records.[3] Also, every state which is

---

[7] *accessnow.org.*

[1] CONGRESSIONAL RESEARCH SERVICE, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality* (Feb. 4, 2014), available at *https://digital.library.unt.edu/ark:/67531/metadc282348/m1/1/high_res_d/RL30318_2014Feb04.pdf.*

[2] NATIONAL CONSUMER LAW CENTER, State by State Summaries of State UDAP Statutes (Jan. 10, 2009), available at *https://www.nclc.org/images/pdf/udap/analysis-state-summaries.pdf* (the overlap between state Unfair and Deceptive Acts and preemption of state privacy laws is when the deceptive or unfair conduct involves the collection, use, or disclosure of personal information. Congress has already witnessed this unforeseen consequence when it passed the Homeowners Protection Act to address homeowner challenges with private mortgage insurance and granting them rights to terminate insurance with disclosure obligations. The wide reaching preemptive language within the Federal law was seen by the courts as a bar on states prosecuting deceptive conduct by mortgage service companies, effectively eliminating state protections against deceptive conduct for that industry). *See* Fellows v. CitiMortgage, Inc., 710 F. Supp. 2d 385.

[3] AMERICAN LIBRARY ASSOCIATION, *State Privacy Laws Regarding Library Records,* available at *http://www.ala.org/advocacy/privacy/statelaws* (Nearly every state has laws assigning confidential status to library records with the exception of Hawaii and Kentucky. However in those two states the state AG has issued opinions outlining protection around library user privacy).

represented by the Senate Commerce Committee has various common law privacy rights that courts have recognized,[4] and that some state legislatures have codified.[5]

To better understand the harmful consequences of the preemption being proposed by certain industry groups, it is valuable to take a closer look at three of the state privacy laws that would be preempted. California's recent Consumer Privacy Act protects all manner of personal information and applies to all manner of businesses. Vermont's recent Data Broker Act focuses on third-party data mining, where the business collecting the information has no direct relationship with the consumer. It is the first state law directed at the data broker industry since the Equifax breach that harmed 145 million Americans. Lastly, the decade-old Illinois Biometric Information Privacy Act requires businesses to get a person's opt-in consent before they gather and monetize their biometrics. The people of these and other states would suffer if Congress enacts a weak consumer privacy law that preempts these stronger consumer privacy laws.

California's Consumer's Privacy Act

Earlier this year, California enacted a far-reaching consumer privacy statute called the Consumer Privacy Act (A.B. 375).[6] The following are among its key protections:

- Consumers have a "right to know" what personal information a business has collected about them, and where (by category) that personal information came from or was sent. *See* Sections 100, 110, 115.
- Consumers have a right to delete information that a business collected from them, with exceptions, including for the First Amendment. *See* Section 105.
- Consumers have a right to opt-out of the sale of personal information about them. *See* Section 120.
- Consumers have a right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act, though with significant exceptions. *See* Section 125.

The Act defines "consumer" as any natural person who resides in California. *See* Section 140(g). In order to exempt small businesses, it defines a "business" as a for-profit entity with $25 million in revenue, with personal information from 50,000 consumers, or with half of its revenue from sale of personal information. *See* Section 140(c).

The California Attorney General will be responsible for enforcing the Act, and for promulgating regulations about it. *See* Sections 155, 185. The Act creates a limited private cause of action for consumers against businesses for data breaches, based on California's existing data breach notification law. *See* Section 150.

---

[4] The following states represented by the committee have judicially recognized common law privacy rights: Alaska (Greywolf v. Carroll, 151 P.3d 1234, 1244–45 (Alaska 2007)), Colorado (Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1066–67 (Colo. App. 1998)), Connecticut (Carney v. Amendola, No. CV106003738, 2014 WL 2853836, at *17 (Conn. Super. Ct. May 14, 2014)), Florida (Allstate Ins. Co. v. Ginsberg, 863 So. 2d 156, 162 (Fla. 2003)), Hawaii (Mehau v. Reed, 869 P.2d 1320, 1330 (Haw. 1994)), Illinois (Lawlor v. N. Am. Corp. of Ill., 983 N.E.2d 414, 424–25 (Ill. 2012)), Indiana (Cullison v. Medley, 570 N.E.2d 27, 31 (Ind. 1991)), Kansas (Werner v. Kliewer, 710 P.2d 1250, 1255 (Kan. 1985)), Michigan (Tobin v. Mich. Civil Serv. Comm'n, 331 N.W.2d 184, 189 (Mich. 1982)), Minnesota (Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 233–35 (Minn. 1998)), Mississippi (Plaxico v. Michael, 735 So. 2d 1036, 1039 (Miss. 1999)), Missouri (Sofka v. Thal, 662 S.W.2d 502, 510–11 (Mo. 1983)), Montana (Rucinsky v. Hentchel, 881 P.2d 616, 618 (Mont. 1994)), Nevada (City of Las Vegas Downtown Redevelopment Agency v. Hecht, 940 P.2d 127 (Nev. 1997)), New Hampshire (Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003)), New Mexico (Moore v. Sun Publ'g Corp., 881 P.2d 735, 742–43 (N.M. Ct. App. 1994)), Oklahoma (Munley v. ISC Fin. House, Inc., 584 P.2d 1336, 1339–40 (Okla. 1978)), South Dakota (Kjerstad v. Ravellette Publ'ns, Inc., 517 N.W.2d 419, 424 (S.D. 1994)), Texas (Valenzuela v. Aquino, 853 S.W.2d 512, 513 (Tex. 1993)), Utah (Cox v. Hatch, 761 P.2d 556, 563–64 (Utah 1988)), Washington (Mark v. Seattle Times, 635 P.2d 1081, 1094 (Wash. 1981) (en banc)), and West Virginia (Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70, 85 (W. Va. 1984)).

[5] The following states have codified the common law right to privacy: Massachusetts (MASS. ANN. LAWS ch. 214, § 1B (LexisNexis 2011)), Nebraska (NEB. REV. STAT. ANN. § 20–203), and Wisconsin (WIS. STAT. ANN. § 995.50(2)(a) (West 2007)).

[6] California Consumer Privacy Act of 2018, (signed into law Jun. 28, 2018), available at *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.*

Illinois' Biometric Information Privacy Act

A decade ago, Illinois enacted our Nation's strongest statutory protection of biometric privacy: the Illinois Biometric Information Privacy Act, 740 ILCS 14.[7] At its core, the Illinois law forbids private entities from acquiring or disclosing a person's biometric information, absent their informed, opt-in consent. *See* Section 15(b) & (d). This empowers people to autonomously decide for themselves whether it is in their best interests to share their biometric information with others.

The Illinois statute also limits the time that a private entity may store a person's biometric information, *see* Section 15(a); bars the sale of biometric information, *see* Section 15(c); and requires entities that hold biometric to securely store it, *see* Section 15(e).

The Illinois law empowers persons aggrieved by violations of the Act to bring a private cause of action against the offending parties. *See* Section 20.

Vermont's Data Broker Act

Earlier this year, Vermont enacted its Data Broker Act (H. 764).[8] The following are its key protections of consumers from data brokers:

- Data brokers must annually register with the state. When they do so, they must disclose information of value to consumers, including: whether there is a way for consumers to opt-out of data collection, retention, or sale, and if so, how they may do so; whether the data broker has a process to credential its purchasers; and whether it has had any data breaches. *See* Section 2446.
- Data brokers must securely store the personal information they acquire. *See* Section 2447.
- Data brokers may not collect personal information by fraudulent means, or for the purpose of harassment or discrimination. *See* Section 2433.
- Credit reporting agencies must provide consumers a free "credit freeze" as a protection against data thieves who attempt to commit credit fraud against breach victims. Many creditors will not extend credit absent a report from a credit agency. If the consumer has previously obtained a "credit freeze," the credit agency will not issue the report, and the creditor in turn will not extend credit to the fraudster. Vermonters now can freeze their credit at no cost, and when they actually want credit, they can unfreeze their credit at no cost. *See* Section 2480b & Section 2480h.

Vermont's Attorney General is empowered to enforce these rules. Individual Vermont residents may bring a private cause of action to enforce the data security mandate and the ban on fraudulent acquisition.

EFF Urges Caution Before Acting

This letter is by no means an exhaustive list of the potential privacy harms that could be done by preemption, but it is meant to convey the gravity of what is being asked of Congress. Many of the companies that are intentionally seeking to monetize information about everything we do online and elsewhere do not intend to ask for laws that actually restrain their business plans. The Committee should understand that the only reason many of these companies seek congressional intervention now, after years of opposing privacy legislation both federally and at the states, is because state legislatures and attorney generals have acted more aggressively to protect the privacy interest of their states' residents, in many cases over their objections. Indeed, 91 percent of Americans believe they have lost control over how their personal information is collected and used[9] with many Americans choosing to avoid using the Internet for various activities due to privacy concerns.[10]

The latest series of national data privacy scandals (many of which have been investigated by this Committee and others) has forced the industry to recognize that state legislators want to protect the privacy of their constituents, and grant them

---

[7] 740 ILCS 14 (Biometric Information Privacy Act), available at *http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.*

[8] 9 V.S.A. Ch. 62 as amended by the 2018 Acts 171 available at *https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf.*

[9] PEW RESEARCH CENTER, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns,* available at *http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.*

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

legal rights, including a right to be made whole after an egregious breach of their personal information through a private right of action.

If Congress wishes to enact legislation that genuinely improves the data privacy of Americans, EFF urges Congress to include the following as part of the baseline:

- Opt-in consent to the collection, use, and disclosure of personal information by online services.
- A "right to know" what personal information companies have gathered about us, where they got it, and with whom they shared it.
- "Data portability," meaning the power of users to take their data, in a usable form, from a company and bring it elsewhere. This will ensure users can vote with their feet should they find a particular practice unacceptable and will promote competitive forces to address privacy concerns.
- A right to equal service, without change in price or quality, for users who exercise these rights.
- A private right of action for users to bring to court companies that violate these rights.

There is much that Congress might do to help protect data privacy. But weak Federal legislation that preempts stronger state legislation would be far worse than doing nothing.

Sincerely,

Electronic Frontier Foundation.

CC: Members of the Senate Commerce Committee

September 24, 2018

Senator JOHN THUNE, Chairman,
Senator BILL NELSON, Ranking Member,
Committee on Commerce, Science, and Transportation,
Washington, DC.
Via e-mail

Dear Members of the Senate Commerce Committee:

Senator Thune set the tone for the upcoming hearing by stating that *"Consumers deserve clear answers and standards on data privacy protection."* Given the scale and social impact of the technical systems being deployed by Google and other corporations, I would add that greater oversight and accountability of not only data, but also the systems that are designed and deployed based on such data, is urgently needed.

Until the beginning of this month, I worked in Google's Research and Machine Intelli-gence division as a Senior Research Scientist, where one of my primary responsibilities was improving Google's search accuracy across a wide variety of languages.

I was compelled to resign my position on August 31, 2018, in the wake of a pattern of unethical and unaccountable decision making from company leadership. This cul-minated in their refusal to disclose information about Project Dragonfly, a version of Google Search tailored to the censorship and surveillance demands of the Chinese government. Like most of the world, including most Google employees, I learned about this effort on August 1, 2018, from public reporting.

It is notable that Project Dragonfly was well underway at the time the company released its AI Principles. As has been widely understood, by human rights organizations, investigative reporters, Google employees, and the public, Project Dragonfly directly contradicts the AI Principles' commitment to not *"design or deploy"* any technology whose purpose *"contravenes widely accepted principles of [. . .] human rights"*.

Some of the most disturbing components of Project Dragonfly, which I here directly verify, include:

- A prototype interface designed to allow a Chinese joint venture company to search for a given user's search queries based on their phone number.
- An extensive censorship blacklist developed in accordance with Chinese government demands. Among others, it contained the English term 'human rights', the Mandarin terms for 'student protest' and 'Nobel prize', and very large numbers of phrases involving 'Xi Jinping' and other members of the CCP.
- Explicit code to ensure only Chinese government-approved air quality data would be returned in response to Chinese users' search.

- A catastrophic failure of the internal privacy review process, which one of the reviewers characterized as actively subverted.[1]

Each of these details was internally escalated by other employees to no avail, and many of them were discussed extensively on internal mailing lists; I understand that such discussion has since been increasingly stifled. I cannot speak for those who escalated these concerns, but I share their fear of the possible consequences.

I am part of a growing movement in the tech industry advocating for more transparency, oversight, and accountability for the systems we build. The primary goals are laid out in the Google Ethics Code Yellow Petition, which not only continues to circulate throughout Google but has also been endorsed by 14 human rights organizations and several technology experts.

I humbly ask that The Committee on Commerce, Science, and Transportation call on Google's representative for the hearing, Mr. Keith Enright, to respond to the sincere and credible concerns of the coalition of 14 human rights organizations who drafted an August 28th Open Letter To Google. I also ask the committee to inquire about how Google is meeting its commitments to privacy under its own AI Principles and the Global Network Initiative, of which Google is a member.

Dragonfly is part of a broad pattern of unaccountable decision making across the tech industry. It has been made clear, both by word and by action, that the leadership at Google will be clamping down on the types of internal investigation that were necessary to bring Project Dragonfly to light. I would hope that The Committee would help protect the environment needed for future whistleblowers by taking steps to guarantee ethical transparency and oversight across Silicon Valley.

Sincerely,

/S/ Dr. Jack Poulson.

CONSUMER FEDERATION OF AMERICA
Washington, DC, September 25, 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 September 26, 2018 on "Examining Safeguards for Consumer Data Privacy"

Dear Chairman Thune and Ranking Member Nelson:

Please accept the following comments for the record from Consumer Federation of America (CFA), an association of nearly 300 nonprofit consumer organizations across the United States. CFA was established in 1968 to advance the consumer interest through research, advocacy and education.

We welcome Congressional hearings to explore privacy issues. Consumers' perspectives are essential to having an informed discussions of those issues, however, and we regret that they are not included in this hearing.[1] While we look forward to additional hearings that will include those voices, it would have been useful to provide an opportunity for corporate and consumer representatives to respond to each other's views.

Our view is that comprehensive Federal legislation on privacy should only be undertaken if it is based on the premise that Americans have an inherent right to privacy[2] and if it will require respect for that right to be integral to the development of commercial products and practices.

---

[1] This privacy review process developed inside Google following years of privacy failures, including the collection of payload Wi-Fi data and registering users for the Google Buzz product without their consent. With this in mind, I would like to point The Committee's attention to the 2011 settlement Google made with the FTC to: (1) submit to an independent review of its privacy practices every two years, (2) receive consent from users anytime its services change in a manner that results in sharing more information, and (3) establish and maintain a "comprehensive privacy program" for the next 20 years. Cf. *https://arstechnica.com/tech-policy/2011/03/google-agrees-to-new-privacy-rules-as-part-of-buzz-settlement/*

[1] CFA joined other consumer and privacy groups in a letter to Chairman Thune in this regard, see *https://consumerfed.org/wp-content/uploads/2018/09/privacy-groups-voice-concern-over-consumer-group-exclusion.pdf.*

[2] Described so aptly more than a century ago by Samuel D. Warren and Louis D. Brandeis in their seminal article, "The Right to Privacy," Harvard Law Review, Vol. 4, No. 5 (December

In far too many cases, Americans' personal information is exploited, not protected. We see debacles such as the Cambridge Analytica case, in which consumers' data was used for secondary purposes they never imagined or desired [3] and the Equifax data breach where there did not seem to be a process for ensuring the security of highly sensitive information about millions of Americans.[4] We see tactics by Google and others to mislead and manipulate individuals into consenting to privacy-invasive default settings.[5] And we see the failure of the Federal Trade Commission (FTC) to take adequate measures to protect Americans' privacy from the corrosive effects of the increasing marketplace dominance of major tech companies.[6]

Yet rather than suggesting ways to address these problems and make real strides to improve the privacy and security of Americans' personal information, many in industry seem to be arguing that we should go backwards, to a time before the General Data Protection Regulation (GDPR)[7] in Europe, before the California Consumer Privacy Act,[8] before laws were enacted in Illinois and Texas protecting the privacy of biometric information,[9] before Nevada required notice of the information collected about individuals online,[10] and before the states enacted data breach laws.[11] They want weak Federal legislation that would preempt the states and fail to give individuals meaningful control of their personal information or hold companies adequately accountable for its misuse. They want the "free flow of data" across national borders but fail to acknowledge that the United States has fallen behind the rest of the world when it comes to privacy protection.

The GDPR is not going away, and Committee members should ask the companies that will testify at the hearing what steps they have taken to implement it for their operations in Europe, whether they are treating consumers in the U.S. the same way, and if not, why? If they are concerned about the "balkanization" of privacy requirements, why not adopt the highest standard everywhere they do business?

Another question to ask is whether the United States should have a Federal agency that can promulgate privacy regulations and has effective enforcement powers, as other countries do. We repeatedly hear from industry that one size does not fit all but that everyone should have to comply with privacy requirements. There are many different types of businesses and their collection and use of individuals' personal information varies widely. Yet, with the exception of personal information collected online from children, the FTC is unable to craft rules to provide guidance for how individuals' personal information should be handled and no civil penalty authority. Indeed, the FTC's ability to deter unfair and deceptive conduct in privacy and security matters has been under attack, and among the arguments that have been made is that the agency failed to specify exactly what companies were expected to do.[12] The only way to develop the guidance that businesses need within an overall privacy framework is to mandate that the FTC or an independent data protection agency promulgate rules for them to follow.

15, 1890), pp. 193–220, available at *http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf*.

[3] *See* Kevin Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," New York Times, March 19, 2018, available at *https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html*.

[4] *See* Lily Hay Newman, "EQUIFAX OFFICIALLY HAS NO EXCUSE," Wired, September 14, 2017, available at *https://www.wired.com/story/equifax-breach-no-excuse/*.

[5] *See* June 27, 2018 letter from consumer and privacy groups to the FTC, available at *https://consumerfed.org/wp-content/uploads/2018/06/deceived-by-design-letter-to-ftc.pdf* calling for investigation after the release of a report, "Deceived by Design," from the Norwegian Consumer Council.

[6] *See* consumer and privacy group comments to the FTC in regard to "The intersection between privacy, big data and competition," August 20, 2018, available at *https://consumerfed.org/wp-content/uploads/2018/08/consumer-privacy-groups-comment-on-intersection-between-privacy-big-data-and-competition.pdf*.

[7] See text at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679*.

[8] As recently amended, text available at *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121*.

[9] Texas Business and Commercial Code §503.001 at *https://codes.findlaw.com/tx/business-and-commerce-code/bus-com-sect-503–001.html;* Illinois Biometric Privacy Information Act, 740 ILCS 14/at *http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57*.

[10] NRS 603A.300–360, *https://www.leg.state.nv.us/NRS/NRS–603A.html#NRS603ASec220*.

[11] The National Conference of State Legislatures maintains a list at *http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*.

[12] See CFA's August 20, 2018 comments to the FTC about its lack of remedial authority in response to its examination of meeting 21st century consumer protection challenges, at *https://consumerfed.org/testimonial/cfa-urges-ftc-to-seek-legal-reforms-to-improve-its-ability-to-meet-21st-century-consumer-protection-challenges/*.

The document "Developing the Administration's Approach to Privacy"[13] which the National Telecommunications and Information Administration will formally release for comment tomorrow fails to recognize privacy as a fundamental right and instead echoes the position of the Chamber of Commerce and others that privacy is a risk to be managed. It endorses the current model of "notice and consent" without addressing the fact that in many cases Americans find that "consent" means "take it or leave it" if they want to use the products and services that are offered them, and it merely restates many common fair information principles without describing how they should be implemented in practice.

If Congress wants to undertake a serious effort to protect Americans' privacy and encourage business models to be built on respect for this vital principle, it should consider legislation that guarantees individual privacy rights, ensures their just and fair treatment, places specific obligations and responsibilities on entities that handle their data, affirms the Federal government's role in protecting it, and gives an agency sufficient authority and resources to do the job. Furthermore, Congress should not interfere with states' abilities to provide stronger protections for their constituents when needed.

Sincerely,

SUSAN GRANT,
Director of Consumer Protection and Privacy,
Consumer Federation of America.

AMERICAN CIVIL LIBERTIES UNION
Washington, DC, September 25, 2018

Re: ACLU Letter on Senate Commerce Committee hearing, "Examining Safeguards for Consumer Data Privacy"

Dear Senator,

On behalf of the American Civil Liberties Union ("ACLU"), we submit this letter for the record in connection with the Senate Commerce Committee hearing, "Examining Safeguards for Consumer Data Privacy," which will examine current data privacy laws and discuss possibly approached to further safeguarding consumers.

We are disappointed that the committee has chosen to move forward with this hearing without representation from any groups that represent consumer interests. We urge the committee to promptly hold additional hearings including representatives of consumer groups regarding what additional laws and regulations are needed to safeguard the public's privacy.

In the last year, we have seen countless data breaches, sharing of sensitive data without consent, and reports that companies have misled consumers regarding their data practices. These privacy violations have jeopardized the rights of millions of Americans and threatened our national security. It is past time for Congress to right the imbalance in our laws that has failed to protect consumers from industry practices that strip them over control of their data in the interest of profit. The central voice in this debate should be consumers. While it certainly fair to hear from industry regarding how regulations may impact their practices, they should not be the first or only voice to weigh in on how to safeguard consumer privacy. This is particularly important given that many industry proposals have been strongly opposed by consumer groups and would in fact weaken even existing privacy laws.

Many industry groups have pressed for Federal legislation that preempts state law.[1] *The ACLU strongly opposes such preemption.* Preemption would come at an unacceptable cost for consumers. It could nullify existing laws, undermine existing enforcement and redress actions, and prevent states from taking steps to protect consumers from emerging privacy threats. This is particularly alarming because it has often been states—not the Federal government—that have acted in a timely and important way to protect consumer interests.

States as diverse as Idaho, West Virginia, Illinois, and California currently have privacy legislation. For example, California was the first state to require companies to notify consumers of a data breach.[2] While other states have since followed suit, the Federal government has yet to enact a strong data breach law. California has

---

[13] Docket No. 180821780–8780–01, RIN 0660–XC043, available at *https://s3.amazonaws.com/public-inspection.federalregister.gov/2018–20941.pdf.*

[1] *See* U.S. Chamber of Commerce, *U.S. Chamber Privacy Principles,* (Sept. 6, 2018), available at https://www.uschamber.com/issue-brief/us-chamber-privacy-principles; Internet Association, *Privacy Principles,* available at *https://internetassociation.org/positions/privacy/*

[2] *See* California Civil Code s.1798.25–1798.29

also required that companies disclose through a conspicuous privacy policy the information they collect and share with third parties, benefitting consumers throughout the country.[3] Similarly, Illinois has set important limits on the commercial collection and storage of biometric information, which has impacted many companies' practices nationwide.[4] Idaho, West Virginia, Oklahoma, and many other states have other laws that protect student privacy.[5] Preemption could adversely impact many of these existing laws, and could foreclose future laws that protect consumers.

Rather than preempting state law, the ACLU urges Congress to enact Federal legislation that serves as the floor—not the ceiling—for laws that protect consumers. Among other things, such legislation should include requirements that companies obtain informed consent to share, use, or retain information; provide data portability; ensure the consumers have clear and conspicuous information about data practices; and adopt appropriate cybersecurity practices. It should also address civil liberties and civil rights concerns associated with automated decision making practices and ad targeting, and limit so-called "pay for privacy schemes" or provisioning use of a service on consent to collect information unnecessary for the provision of such a service. Finally, any Federal legislation must be accompanied by strong enforcement mechanisms and a private right of action for consumers who have their privacy violated.

Many of these proposals are not ones that have been put forward by industry, which further underscores the need to ensure that consumer voices are a central part of the debate over Federal privacy legislation. If you would like to discuss these issues in more detail, please contact Senior Legislative Counsel, Neema Singh Guliani at *nguliani@aclu.org.*

Sincerely,

FAIZ SHAKIR,
National Political Director.
NEEMA SINGH GULIANI,
Senior Legislative Counsel.

PUBLIC KNOWLEDGE
Washington, DC, September 26, 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 "Examining Safeguards for Consumer Data Privacy."

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 dis-

---

[3] *See* California Code, Business and Professions Code—BPC § 22575

[4] *See* Biometric Information Privacy Act, 740 ILCS 14/, *http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57*

[5] *See* Center for Democracy and Technology, *State Student Privacy Law Compendium* (October 2016), available at *https://cdt.org/files/2016/10/CDT-Stu-Priv-Compendium-FNL.pdf*

[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.*

crimination."[4] Against this backdrop, the Committee's consideration of appropriate safeguards for consumer data privacy could not be timelier.

Consumer voices are critical to the privacy debate, and while we are pleased that the Committee has committed to holding additional privacy hearings, we are disappointed consumer and privacy advocates were not invited to participate in this particular hearing. Nonetheless, we appreciate 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 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

---

[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).

[10] *See supra* notes 1–3.

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]

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

---

[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.")

[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/*.

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.

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

---

[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).

[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).

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. In addition, 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 engaged 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.

---

[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).

[25] 47 U.S.C. § 551(f)(2)(A) (2001).

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 *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.

---

[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.*

[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.*

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 anticipate that this hearing is part of a longer conversation about consumer data privacy. We appreciate the opportunity to submit this statement for the record and stand ready to assist the Committee in preparation for future hearings and as it crafts and considers possible legislative solutions. 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

---

October 1, 2018

Chairman JOHN THUNE,
Ranking Member BILL NELSON,
Senate Commerce Committee,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson,

We appreciate your interest in consumer privacy and the hearing you convened recently to explore this topic.

Still, our concerns remain that the hearing, with only industry representatives, was unnecessarily biased. Many of the problems consumers face, as well as the solutions we would propose, were simply never mentioned. There is little point in asking industry groups how they would like to be regulated. None of the proposals endorsed by the witnesses yesterday would have any substantial impact on the data collection practices of their firms. Such regulation will simply fortify business interests to the detriment of online users. And the absence of consumer advocates at the first hearing was also missed opportunity for a direct exchange about points made by the industry witnesses.

We understand that you are planning to hold a second hearing in early October. In keeping with the structure of the first hearing, we ask that you invite six consumer privacy experts to testify before the Committee. We would also suggest that you organize an additional panel with other experts and enforcement officials, including Dr. Jelenik, the Chair of the European Data Protection Board, as well as State Attorneys General, who are now on the front lines of consumer protection in the United States.

---

[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).

Thank you for your consideration of our views. We look forward to working with you.

Sincerely,

Access Humboldt
Access Now
Campaign for a Commercial-Free Childhood
Center for Digital Democracy
Common Sense
Consumer Action
Consumer Federation of America
Customer Commons
Digital Privacy Alliance
Electronic Frontier Foundation
EPIC
Media Alliance
National Association of Consumer Advocates
New America's Open Technology Institute
New York Public Interest Research Group (NYPIRG)
Privacy Rights Clearing House
U.S. Public Interest Research Group (U.S. PIRG)
World Privacy Forum

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO LEN CALI

Question 1. In general we have been exploring the idea of opt in frameworks to keep consumers informed about what their data is being used for. However, we know from recent history that there are some uses of data that should never be permitted—like the leveraging personal data to interfere with election processes. How could we design an opt in framework that is meaningful to consumers, doesn't desensitize them to important decisions about privacy and makes sure they consent only to lawful uses of their data?

Answer. There are harms associated with a comprehensive opt-in regime for all uses of data. One such harm, as you noted, is desensitizing consumers to privacy concerns. An all "opt-in" regime also risks stifling innovative uses of data that benefit consumers.

It is worth noting that the GDPR does not impose a blanket opt-in requirement, but rather allows companies to rely on "legitimate interest" and other legal bases to process consumer data. Likewise, the FTC has recognized that sensitive data—*i.e.,* Social Security numbers and financial, health, children's and precise location information—deserves added protection, such as requiring opt-in consent for external sharing of that data for marketing purposes. However, other types of non-sensitive data, such as device or ad identifiers or de-identified location information, do not present the same risk of consumer harm and could provide great benefit, such as with a traffic mapping app. Additional consent generally is not required to use non-sensitive data, provided that companies are transparent with consumers about their data collection and use practices and allow consumers to opt-out of certain uses.

This flexible, risk-based approach has provided customers strong protection without stifling innovative and responsible uses of data. In addition, this approach has avoided a cumbersome European model, which often presents customers with "pop up" consents for each website they visit. That approach runs the risk of desensitizing consumers to important privacy decisions. In short, opt-in privacy requirements should be limited to use of sensitive data.

Finally, we agree that there are some uses of data that should be restricted. Current law, for example, would prohibit uses of data to unlawfully discriminate against persons on the basis of race for employment, housing or issuing credit. Rather than impose opt-in requirements on all uses of data, Congress would do better by identifying the subset of data that may warrant heightened protections and prohibiting certain specified uses of data that should be unlawful.

Question 2. Short of regulation, what more can you and your colleagues and competitors do to restore and maintain our and our constituents' trust that you won't continue to collect more data than consumers understand, use it in ways they never imagined, and then fail to protect the data from unauthorized use and access?

Answer. We agree with you that that each company collecting consumer data has a responsibility to secure and use it in a manner that maintains consumer trust. To keep this trust, our privacy program is based on a core set of principles that explain our commitments to transparency, respect, consumer choice and control, and security.

- Our privacy policies describe the data we collect and how we use it. We also detail how we share consumer information and how consumers can exercise choice and control over how their information is used.
- Our privacy principles are reflected in our values. For example, the AT&T Code of Business Conduct (COBC) requires covered employees to follow the laws,

rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and security and privacy of our customers' records. We take this seriously, and employees who fail to meet our standards are subject to disciplinary action, including dismissal.

- We have a Chief Privacy Officer (CPO), who reports directly to our Chief Compliance Officer, who reports directly to our CEO. Our CPO is tasked not only with ensuring that our privacy practices comply with the law and our published policies, but that they also respect our customers.
- In addition, since 2014, AT&T has issued a Transparency Report that identifies the number and types of legal demands for customer information received in criminal, civil, and national security matters, as well as emergency situations. It also includes international demands related to global operations for customer information and website blocking. The Transparency Report is available in Spanish, to better inform our Latin American customers.
- We've implemented technology and security features and policy guidelines to safeguard the privacy of personal information. For example, we maintain and protect the security of computer storage and network equipment; utilize authentication methods to control access to sensitive data; apply appropriate security controls, including encryption, to protect personal information we store or transmit; and limit access to certain information to only those personnel with jobs requiring such access. Moreover, as a communications services provider, we also have a robust cybersecurity program that helps ensure the safety of our customers' information. As an example, AT&T's global network currently transports more than 200 petabytes each day which gives us valuable intelligence about the ever-changing cyberthreat landscape. This intelligence combined with automated threat detection technologies enables AT&T to safeguard not only the network and our own infrastructure, but also our customers' data, as the sheer volume of cyberattacks continues to grow significantly. AT&T's internal security policy is based upon widely accepted, international security standards such as ISO 27001, PCI, SAS/70, and NIST 800–53, and is consistent with the NIST Cybersecurity Framework.

Finally, AT&T also participates in voluntary privacy programs and standards developed through collaborative public-private collaboration, such as the Digital Advertising Alliance's (DAA's) Advertising Choice program. These voluntary programs could be the basis of enforceable commitments to privacy standards, thereby fostering trust. Congress could establish safe harbors and other incentives to encourage companies to participate in these types of industry privacy programs.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO LEN CALI

Question 1. Several public interest organizations have written the Committee in advance of the hearing expressing their deep concerns about state preemption. As the ACLU noted, it has often been the states—not the Federal Government—that have acted in a timely and important way to protect consumer interests.

Please provide to me a set of recommendations for how to improve the California Consumer Privacy Act and the GDPR.

Answer. GDPR and the California Privacy Act (CCPA) are highly prescriptive and ambiguous, and there are a number of open questions on how their requirements will ultimately be enforced. The California law, which was passed hastily, risks causing a number of unintended consequences, such as: eliminating popular consumer loyalty programs, creating litigation and damages for breaches that do not cause consumer harm, and requiring confusing state-specific disclosures on websites. We are particularly concerned with how the bill's access requirements will be interpreted and enforced, particularly given the seemingly absolute nature of some of these obligations. CCPA's overly broad definition of personal information also raises questions about whether and how businesses can de-identify data, something Congress should incentivize companies to do. The broad definition, particularly the inclusion of the term "household," also raises questions of how companies can comply with CCPA without violating the privacy of others. GDPR, which took effect in May, has already had negative effects, reportedly causing hundreds of websites to go dark across the EU. A Federal privacy law should adopt clear, risk-based restrictions so as not to deny consumers the benefits of responsible data use.

While in our Federal system, consumer protections often vary by state, these variations make less sense where data moves freely, without regard to borders and at

the speed of light. Consumers deserve a single set of privacy rules that they can understand and rely upon across the Nation. A patchwork quilt of differing Federal and state privacy laws would confuse consumers, would be unworkable for business and would stifle innovation.

In addition, there is every reason to believe that the FTC would aggressively protect consumer interests under a new Federal privacy law. It has brought more than 500 enforcement actions for privacy and data security violations, including cases involving major Internet and telecommunications companies. The FTC has been the Nation's preeminent privacy "cop on the beat" and a Federal privacy law should build on and strengthen the FTC's role.

Question 2. Between the six of your companies, you have access to an overwhelming amount private information about nearly everyone in the United States. AT&T and Charter have access to the browsing history of your customers. A Princeton study found that Google collects visitor data from 70 percent of websites—including from Twitter, a competitor. It's hard to imagine what your companies don't know.

Answer. We agree that collection of information is widespread. ISPs, such as AT&T and Charter, collect information, though to a lesser extent than your question presupposes. For example, encryption of data as it travels between the mobile device and a website or proxy service mask more than 80 percent of the Internet access traffic coming through AT&T's facilities. This percentage is growing.

Question 3. Would you commit to privacy-by-design—limiting collection of data and deleting data when it is no longer useful to your customers?

Answer. AT&T has long practiced "privacy by design," and we promote privacy throughout our company and in our development of our products and services. For example, new products and uses of data are subject to a privacy impact assessment to determine its compatibility with legal requirements and AT&T's privacy policies. Our privacy policies explain that we collect and retain data for a variety of purposes that benefit our customers, such as delivering service, maintaining and improving service quality, securing our network and our customers, and, as appropriate, for marketing and business analytics.

Question 4. What specific steps do you plan to take to limit your own use of customer data? Can you provide examples where you deleted or stopped collecting data to protect privacy?

Answer. AT&T reviews its data collection and use practices as part of examining the privacy impact of new services and business use cases. We also review our data retention practices on an ongoing basis, taking into account the needs of the business, as well as tax and legal requirements.

Question 5. Privacy by design is fundamental to the GDPR. What specific changes have you made to your products to come into compliance to the GDPR's privacy-by-design requirements?

Answer. As noted in response to Question 2, AT&T has long practiced "privacy by design," and we promote privacy throughout our company and in our development of our products and services. In respect to GDPR, as an example, AT&T's communications entity has enhanced its existing privacy program, including our Privacy Impact Assessment process by mechanizing and developing tools to complete the data protection impact assessments required by GDPR. Our communications company, which does not have consumer facing operations in the EU/EEA, has enhanced its training, contracting, documentation, procedures and technologies with a focus on EU/EEA B2B customer and AT&T employee personal data.

Question 6. In most of your remarks, you discuss the challenges of regulating evolving technologies and economies. It would seem to me that this requires a Federal agency that is responsive to technology changes.

Would you support the FTC having rulemaking authority to provide clarity, to address potential harms, and to ensure rules match technology changes? What sorts of areas should this cover?

Answer. Rulemakings are only one way that an agency can provide predictability and guidance. In the context of privacy, the FTC has historically provided clarity by issuing guidance and reports that respond to evolving technologies and market conditions. Moreover, a carefully crafted statute should be able to capture future technological and market developments without providing an agency undue discretion to alter the congressional framework. A clear set of statutory requirements would provide consumers and industry greater certainty over time than rules subject to change by an agency. This is important because rulemaking authority, if unguided, could lead to fewer consumer choices than Congress might intend and could chill responsible and innovative uses of data that would benefit consumers. While there are circumstances where properly proscribed rulemaking authority may

be appropriate—and it would be wise to allow the FTC flexibility to reduce statutory restrictions as circumstances warrant—Congress should establish a high bar before the FTC may restrict consumer and business choices beyond those explicitly established by Congress and should define clear parameters within which the FTC may operate to implement and enforce the law.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TOM UDALL TO LEN CALI

Question. Unsurprisingly, none of your testimony speaks about potential increased penalties for a new privacy framework. The current penalty regime seems not to change corporate behavior—as we repeatedly have seen. In your opinion, are civil penalties an effective mechanism to push companies to follow the law? If not, what mechanisms would be effective?

Answer. Using its existing authority, the FTC has established its privacy and data security framework, which has been widely implemented by companies across different industries. The FTC has aggressively enforced this framework under its existing authority. For example, the FTC has brought more than 500 enforcement actions for privacy and data security violations, including cases involving major Internet and telecommunications companies. By our count, in 184 instances these FTC enforcement actions resulted in the entry of enforceable consent decrees. Companies have generally complied with those decrees, given the low number of FTC complaints associated with violations. In the event the FTC determines that a company violated a consent decree, the FTC may file a complaint and seek civil penalties. The Commission also has the power to seek restitution and injunctive relief.

A new Federal privacy framework should ensure that the FTC has the resources and tools it needs to effectively enforce this new framework. To comport with due process, any new penalty authority, particularly first offense penalties, should apply only in cases of clear violation of explicit statutory duties or agency rules.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO LEN CALI

Question 1. Positive Aspects of State Laws/GDPR: Your company has called for a national privacy framework in order to avoid a patchwork of state laws which you have to comply with as your data travels across state lines. From an international perspective, Europe has GDPR. You have operations around the country, and some around the globe and have seen firsthand how these laws are being implemented.

Are there any states that you believe have the right framework, or aspects, in place?

Can you point to an aspect of the California law that you believe is reasonable and should be emulated on the national level?

Nevada passed a privacy notice law during the 2017 session, how is your company doing in complying with this?

What part(s) of the GDPR should we look to emulate in the U.S?

Answer. The GDPR and the new California law are overly prescriptive and restrictive. That said, each provide a single, consistent framework applicable to all companies that collect and use data. That is a good outcome and one the U.S. should emulate by adopting a Federal law that establishes consistent, nationwide privacy protections for consumers, instead of a patchwork of inconsistent state laws.

Another positive aspect of the GDPR and the new California privacy law is that they do not impose blanket opt-in requirements. As discussed above, the GDPR allows companies to rely on legitimate interest and other legal bases to process data. The new California privacy law requires an opt-out choice for selling data, but does not restrict how companies collect and use data.

In terms of other states, we would point to the Nevada and Delaware Online Privacy Protection Acts, which provide reasonable, consumer-friendly privacy notice requirements for online service providers.[1] As a communications carrier operating in these states, AT&T is in compliance with these requirements. However, these laws—limited to these states and to online service providers—fail to provide consumers consistent, nationwide privacy protections. That is why a nationwide, Federal law is necessary to maintain consumers' trust by providing them a consistent

[1] Nevada Revised Statutes § 603A.300; Delaware Code § 1205C.

set of privacy protections that apply regardless of where personal information is collected or which device, service or company is collecting and using it.

Question 2. State Attorneys General: I understand the utility of having a national framework given how difficult it would be to develop 50 different frameworks based on state law. At the same time, we want to ensure that states play a role in protecting the privacy of their residents.

What should, in your view, be the role of State AGs in enforcing privacy standards?

Answer. We do not object to providing state attorneys general an appropriately defined role in enforcing Federal privacy standards, subject to the FTC's role as the exclusive Federal and primary regulator and enforcer.

Question 3. Law Enforcement: I believe our law enforcement officials should have a mechanism to obtain the data they need for legitimate investigations. At the same time we need to strike the right balance between keeping our country and communities safe while protecting individuals' civil rights and privacy. Your company has access to many of the personal and intimate choices of millions of your customers, data and records that paint the picture of the everyday lives of millions of American families.

How do you believe a national privacy framework could seek to strike the right balance?

Answer. Congress has the primary role in determining the appropriate body to decide the proper balance between law enforcement's right to access information while protecting individuals' civil rights and privacy. That said, separate from privacy legislation, we support updating government access laws to reflect technology developments. For example, we have supported modernization of the Electronic Communications Privacy Act to require that law enforcement obtain a warrant to access communications content, regardless of the length of time for which it is stored.

To the extent AT&T has records in its custody or control that are subject to a mandatory legal obligation to produce the records, AT&T will comply with the legal requirement. And although we comply with legitimate government demands for customer communications, we do so only to the extent required by law or in exigent circumstances expressly allowed by law.

Question 4. Privacy Enhancing Technology: There are many technologies that actually enhance users' privacy: Encryption, anti-virus, cybersecurity technologies are all examples of this. I think this is a portion of the privacy debate that sometimes gets looked over, but one we should consider as we look at privacy legislation.

Can you summarize some of the privacy enhancing technology used at your company?

Do you believe the Federal Government could assist in either funding the development of similar technologies or establishing a framework for companies to implement them into their data processing?

Answer. Although AT&T expends substantial resources to secure the data of our customers, we also recognize that security practices should not follow a one-size-fits-all approach; rather, such practices should be tailored to the nature of the data, risk of harm and other factors. We've implemented various technology and security features and policy guidelines to safeguard the privacy of personal information. Some examples of such practices include: maintaining and protecting the security of computer storage and network equipment; utilizing authentication methods to control access to sensitive data; applying encryption or other appropriate security controls to protect personal information we store or transmit; and limiting access to certain information to only those with jobs requiring such access (including utilizing mechanisms to manage appropriate access);

The Federal Government can contribute to innovation in and the development of security solutions, which can also help protect privacy, in a several ways. For example, the government can: (1) Fund consumer education initiatives and grant programs that promote development of innovative security solutions; (2) promote government investment in technologies for Federal systems; and (3) develop Federal policies and approaches to security that are risk-based and voluntary (as opposed to prescriptive regulatory approaches). Such initiatives can help promote innovation in cybersecurity and data security technologies and avoid diverting resources away from innovation and security and towards checklist compliance. The government can also help by: (4) convening multistakeholder efforts to research and develop solutions designed to access, query, hold and secure data with privacy in mind; and 5) providing tax, student loan and tuition incentives for students to pursue careers in cybersecurity and for software engineers with cybersecurity expertise to participate in open source software forums.

Question 5. Small Business: As we talk about a national framework, one of the most important things to keep in mind is how we work with small business. Your company has the ability to maintain cybersecurity and compliance teams that make it easier for your companies to work with any potential law we pass.

Can you discuss how your companies might be working with, or aiding, small businesses with their privacy and data needs?

Also, can you provide your thoughts on how a Federal framework would best take the challenges and opportunities of small businesses into account?

Answer. We appreciate the challenges that small businesses face in attempting to comply with regulatory frameworks. A Federal framework would best promote privacy and lessen the burden on small businesses by creating rules based in reasonableness, enforced by a uniform Federal regulator, and tailored to the sensitivity of data collected. In addition, a privacy and security framework based on a reasonableness standard would help limit compliance burdens on small business while promoting heightened protections for the most sensitive types of data.

For our part, AT&T sells managed security services to businesses that help them protect the networks and other platforms that transmit and store their confidential or sensitive information. For example, AT&T NetBond® for Cloud services orchestrates highly-secure network connections to Cloud service provider platform centers and private Clouds which, among other benefits, enhances the security of a business's data as it moves between that business's facilities and its Cloud platform and helps reduce the potential for DDoS attacks and other common cyber threats by directly connecting customers with their Cloud service providers.

Question 6. Data Protection Officers: As you all 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 company's perspective on this requirement?

Answer. We do not object to this requirement. AT&T has long had a Chief Privacy Officer, who reports directly to our Chief Compliance Officer, and who is responsible for overseeing and enforcing the company's privacy policies and commitments. However, as discussed above, Congress should avoid overly prescriptive privacy program requirements that increase the compliance burden without benefitting consumers.

Question 7. Data Minimization: One component of the GDPR is a concept known as "data minimization." This principle states that data processing should only use as much data as is required to successfully accomplish a given task and data collected for one purpose cannot be repurposed without further consent. The idea behind this is both to ensure that users are comfortable that their data is only being used for the purposes which enhance the experience and also help limit the impact of any data breaches.

It seems like there may be challenges to implementing something this broad, especially as it is laid out in the GDPR, but it nonetheless feels like something that should be explored as part of our conversation here in the United States.

What is your company's perspective on this requirement?

Answer. GDPR's data minimization requirements run the risk of being overly restrictive and limiting responsible and innovative uses of data that benefit consumers. In framing national privacy legislation, Congress should adopt a balanced approach that affirmatively recognizes that innovative uses of data also benefit consumers. AT&T suggests that Congress start with the current FTC's risk-based approach, which calibrates privacy safeguards based on the sensitivity of data and how it is used.

In taking this risk-based approach to regulating data use, the FTC has provided consumers strong privacy protections, while allowing companies flexibility to innovate.

Question 8. 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.

Do you build your own data centers or contract with another entity?

What steps do you take to secure these centers?

How often [do] you review your physical data security standards?

Answer. AT&T both owns and leases data centers. We've implemented technology and security controls and policy guidelines designed to safeguard the security of AT&T and customer information. As a communications provider, AT&T has a Chief Security Office (CSO) that publishes a comprehensive, enterprise-wide security policy designed to protect network-related elements, systems, applications, data, and computing devices owned or managed by AT&T. The CSO and other auditing functions regularly review and assess the corporation's security posture to keep pace with industry security practices, including regular updates to security policies. Physical security is no exception. AT&T manages the physical security measures at its facilities through layers of protection depending on the infrastructure and resources at a location. These measures may include, but are not limited to, locked and monitored entrances, on-site security personnel, card readers, video monitoring, and the like.

Question 9. AT&T Data Sharing: In June, and in response to public pressure, AT&T announced it would stop sharing users' location details with data brokers "as soon as practical in a way that preserves important, potential lifesaving services like emergency roadside assistance."

Can you confirm that AT&T has followed through on this?

Answer. Yes, since our announcement, we shut down a number of—and are we are winding down the remaining—location-based aggregator services that do not support emergency or other critical services such as roadside assistance and fraud prevention.

Question 10. What other information do you share with third party data brokers?

Answer. AT&T's privacy policies explain with whom we share customer information and for what purpose. For example, we may share it with third parties that perform services on our behalf, only as needed for them to perform those services. We may share information linked to device identifiers with companies who deliver online advertising. We also share with other companies and entities to: respond to 911 requests and other emergencies; comply with court orders and legal process; assist with identify verification and preventing fraud and identify theft; enforce our agreements and property rights; and obtain payment for products and services.

Question 11. Do you believe the average customer is aware of these practices?

Answer. AT&T is committed to being transparent about its privacy practices. As noted above, AT&T's privacy policies explain our practices, including with whom we share personally identifiable information and for what purpose. In addition, AT&T participates in the DAA's Advertising Choices program, which includes a standardized icon for online ads. Federal privacy legislation would help to ensure that privacy disclosures are more consistent across companies and across the country. Federal privacy legislation that includes consistent requirements is also an important way to ensure that consumers are aware of data collection and use practices.

Response to Written Question Submitted by Hon. Roger Wicker to Andrew DeVore

Question. I'm interested in how Amazon interacts with small businesses or other marketplace sellers that use your platform. In many instances, Amazon is selling products as a direct competitor to small business on its platform. Does Amazon use any data it collects from small businesses or other marketplace sellers using its platform to inform decisions related to the items that Amazon will sell directly to consumers? Please explain.

Answer. Customer trust is of utmost importance to Amazon. More than half of all products sold on Amazon are sold by third-party sellers, and sellers are important customers. Just like any retailer, we have information about the items sold in our store and use it to provide a better customer experience, including analytics to improve efficiencies in fulfillment and shipping and to empower all of our sellers. We provide an array of innovative services, tools, and data to our selling partners to help them sell more, increase their efficiency, and manage their inventory. We also advise them on opportunities to expand their product offerings. Furthermore, data and information such as price, best sellers, product recommendations, and customer reviews are all publicly available, and are used by not only Amazon and our selling partners, but by large and small retail competitors alike.

We are proud of the great success that hundreds of thousands of small and medium-sized businesses have found on Amazon since we opened our store to third-party sellers more than 15 years ago. Our seller partners use Amazon's websites in multiple languages and network of more than 100 fulfillment centers to reach cus-

tomers across the world, and their sales are growing faster than our own retail sales.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO ANDREW DEVORE

Question 1. Your written testimony discussed the concept of "privacy by design" as a solution for incorporating privacy safeguards in the development of the services and products that Amazon offers. Given their "multiple layers," are there concerns or barriers to clearly and succinctly explaining to the consumer what these protections are?

Answer. Customer trust is of utmost importance to Amazon, and we endeavor not only to make our use of data and privacy protections clear to customers in simple and easy to understand terms of use, but in the intuitive presentation and use of our products and services. Just one example of this is the visual indicator that appears on the Echo device to let you know when the wake word has been detected and audio is being streamed to the cloud to operate the service.

Question 2. Efforts to draft meaningful Federal legislation on consumer data privacy will heavily rely upon determinations of what types of personally identifiable data are classified as "sensitive" and what are not. While some have suggested that expanded FTC rulemaking authority is necessary to flexibly account for new types of data sets coming from innovative technologies, I have concerns that excessive rulemaking authority could lead to frequent reclassifications of the types of data with ensuing liability adjustments. Do you have suggestions on how to best identify "sensitive" personally identifiable information?

Answer. Privacy issues are complex, and there is great risk of unintended consequences from privacy regulation that is not carefully crafted to deliver clear privacy benefits. When answering privacy questions we start with the customer and work backwards. As a result, when we collect data customers may perceive as particularly sensitive, we consider whether to take additional steps to mitigate the risk that customers will be surprised or upset by our collection or use of that data.

We similarly believe it is important to focus legislative attention on data that presents a privacy risk to an individual. Sensitive data is personal information that identifies a particular individual or a device that belongs to that individual, either alone or when linked with other sensitive categories of data such as health information, financial information, and any information about an individual aged 13 or younger.

Amazon is a member of the Internet Association (IA) and we encourage policymakers to look to the IA's Privacy Principles available at *https://internetassociation.org/positions/privacy/* as they begin to explore a potential national framework.

Question 3. NTIA issued a request for comment on ways to advance consumer privacy without harming prosperity and innovation. I commend the administration for their attention to this important issue. The "High Level Goals for Federal Action" that NTIA is seeking comments for includes inter-operability and the development of a regulatory landscape that is consistent with the international norms and frameworks in which the U.S. participates. How do you foresee Federal legislation affecting cross-border data flows?

Answer. Privacy issues are complex, and there is great risk of unintended consequences from privacy regulation that is not carefully crafted to deliver clear privacy benefits. When answering privacy questions we start with the customer and work backwards. We appreciate NTIA's recognition that the regulatory landscape needs to be harmonized in order to avoid a contradictory patchwork of obligations that will burden organizations and confuse users. For the United States to lead on privacy, we need a consistent approach to privacy that provides clarity for American consumers and businesses.

We also agree with NTIA that any action addressing consumer privacy should be applied comprehensively across private sector organizations that use personal data. The distinction between "physical" and "digital" is increasingly blurring, and now largely meaningless. What many refer to as the "digital economy" is best understood as a set of technologies now in widespread, if not universal, use throughout the economy in industries as diverse as advertising, agriculture, automotive, manufacturing, and retail. Industries not thought of as "digital" will reap huge benefits, as will society as a whole. Thus, treating tech-enabled businesses or innovation leaders differently makes little sense, particularly as new technology proliferates rapidly across every industry.

Question 4. Also included in NTIA's request for comments, how should the U.S. Government encourage more research and development of products and services that improve privacy protection?

Answer. The U.S. Government has long been the global leader in innovation policy and research and development. Thoughtful policymaking that puts the consumer first will lead to continued innovation in privacy protective products and features that people will enjoy, while a patchwork of regulatory obligations will divert significant resources from developing such features. Privacy regulations that place additional overhead and administrative demands on organizations, potentially displacing research and development, should be required to produce commensurate consumer privacy benefits. We agree with NTIA that being overly prescriptive can result in compliance checklists that stymie innovation, and a patchwork of regulations would exacerbate this problem.

Question 5. 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. We have for many years made it easy for customers to access their personal data, ranging from order history, content and devices, to voice recordings. Personal data varies by customer and may range from purchasing history to address and credit card information to customer service interactions. We provide access to personal and customer information in a manner most customers have found relevant and useful for the services that they use.

Question 6. 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. An algorithm is simply a step-by-step set of directions to accomplish a particular task or achieve an identified outcome. Amazon uses machine learning tools and algorithms across multiple products and service features, and their outputs typically are neither personally identifiable nor sensitive. GDPR recognizes a number of lawful bases for processing EU personal data, including legitimate interest, consent, and contract performance. We have a long-standing commitment to privacy and data security. Privacy is built into our services from the ground up—we design and continually improve our systems with customer security and privacy in mind. We strive to limit, de-identify, or pseudoanonymize data where possible or appropriate for customer services. We comply with GDPR access and deletion according to the lawful bases for processing EU personal data.

Question 7. Since companies often use aggregated data outputs to study and improve their existing algorithms, services, and products, what impacts do you expect these vague GDPR requirements to have on companies' abilities to innovate?

Answer. Our long-standing commitment to privacy aligned us well with the GDPR principles; however, meeting its specific requirements for the handling, retention, and deletion of personal data required us to divert significant resources to administrative and record-keeping tasks and away from inventing new features for customers and our core mission of providing better service, more selection, and lower prices. Although data in aggregated form is not subject to GDPR, companies must often use individually tracked data as an input to achieve aggregated outputs, so the process is subject to all of the restrictions and administrative burdens of GDPR. We encourage Congress to ensure that additional overhead and administrative demands any legislation might require actually produce commensurate consumer privacy benefits.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELLEY MOORE CAPITO TO ANDREW DEVORE

Question 1. According to a study by Pew Research, only 38 percent of consumers know how to limit what information they give online. Consider me among those consumers who do not know what is being collected and how to keep my information to myself. Even with privacy settings and assurances that my data is not being collected and used without my consent, I still have concerns. I believe the root of this issue is transparency and consumer confidence. What are your companies doing to increase the transparency when it comes to the type of data you collect?

Answer. Our customer-centric approach has led Amazon to follow privacy by design principles since our founding. We design our products and services so that it is easy for customers to understand when their data is being collected and control when their data is shared. While written disclosures and policy notices are an important foundation for transparency, we do not rely on disclosures alone when collecting customer data. We strive to make that collection intuitive to the customer based on product functionality, and that collection is directly tied to a concrete customer benefit. Where the collection of data is less likely to be intuitive to the customer, we strive to help the customer understand the data collection with conspicuous messaging, such as an indication that we are collecting the data together with a "learn more" link.

Question 2. What difficulties have your companies faced when developing more transparent privacy policies?

Answer. Creating smart privacy policies and practices takes careful attention, and a strong focus on the customer makes it easier to make good decisions. As new laws take effect, overly prescriptive rules and regulations may have the unintended result of longer, and less transparent, privacy policies.

Furthermore, new inventions like Amazon's Echo can create novel challenges for providing customers transparency and control, requiring invention and innovation to deliver great products that preserve customer trust. We need to ensure any potential new consumer privacy framework does not prevent the ability to invent new mechanisms for consumer transparency and privacy control. With the Echo, we had to invent new transparency techniques for a device that did not have a screen. But, when you start with the customer and work backwards, the correct answer is often right in front of you. With the Echo, we were able to use product design to communicate to customers about data collection. For example, the light ring at the top of the Amazon Echo turns blue to alert the customer that the device has heard the "wake word" and is streaming the customer's voice recording to the cloud.

Question 3. West Virginia has a high elderly population that is rapidly increasing as baby boomers retire. I am positive that a lot of my elderly constituents are among those individuals who do not know how to limit their online information. What are some of the measures your companies are doing to teach consumers—and specifically older consumers—about what data they share on your platforms?

Answer. We design our products and services so that it is easy for all of our customers to understand when their data is being collected and control when their data is shared. We endeavor to provide this transparency not just in the terms of use and account settings for each experience, but in the experience itself. For example, customers can manage their Alexa privacy settings from a single page in the Alexa app and on the Amazon website. This includes the ability to listen to and delete voice recordings associated with their account and control skill permissions.

We are also developing product services and features with all of our customers in mind. For example, customers with disabilities and older customers can especially benefit from Alexa's presence in their lives, and from the greater independence a voice user interface can provide. Our teams are working hard to ensure Alexa devices and the Alexa Mobile app are accessible to these customers and have an easy device setup. We are also working to launch new features enabling Alexa to meet daily customer needs through a combination of building new experiences and extending functionality.

Question 4. I know advertising through data collection has a monetary value, and appreciate the business model, however, I find it hard to know what is being collected and how I can keep my information to myself. Even with privacy settings and assurances my data is not being used without my consent, I still have concerns.

Please explain how your business model allows both data to be used to make suggested recommended purchases on your site? As well as how you use that data to target ads to consumers? And how do you do that while protecting personal data?

Answer. Product recommendations, which help customers discover items they might not otherwise have found, are core to the Amazon shopping experience. Customers see these features in clearly labeled formats like "Frequently bought together" and "Customers who viewed this item also viewed." We use aggregate data from our customers' browsing and purchase behavior in order to make recommendations, such as suggesting baby wipes and tear-free shampoo for a customer purchasing diapers.

At Amazon our entire business is built and based on customer trust and this is also true for our advertising program. We take the privacy of our customers very seriously. All information used to provide customers with interest based ads is anonymized and maintained and used in separate dedicated systems. We provide clear and prominent notice regarding our advertising practices both on our prop-

erties and where possible in ads that we deliver on third party properties. We make it simple for users to opt out of receiving interest based ads from us.

Question 5. How can Congress ensure that data collected is used responsibly without shutting down the collection of data completely?

Answer. Privacy issues are complex, and there is great risk of unintended consequences from privacy regulation that is not carefully crafted to deliver clear privacy benefits. When answering privacy questions we start with the customer and work backwards. Customers should know how their data is being used and be empowered to make their own individual determination of the benefits they gain from choosing to use new services and technologies. We believe that policymakers and companies like Amazon have very similar goals—protecting consumer trust and promoting new technologies. Congress should contemplate a Federal framework that meets individuals' reasonable expectations with respect to how the personal information they provide companies is collected, used, and shared, and their attendant rights; that includes mechanisms for customers' rights and controls that provide commensurate privacy benefits to customers; that is mindful of the impact of regulation on small-and medium-sized companies; and that applies consistently across all entities and segments of the economy.

Amazon is a member of the Internet Association (IA) and we encourage policymakers to look to the IA's Privacy Principles available at *https://internetassociation.org/positions/privacy/* as they begin to explore a potential national framework.

Question 6. In April, the European Union (EU) passed the General Data Protection Regulation (GDPR) in order to protect personal data and uphold individual privacy rights. These new regulations have created uncertainty for U.S. firms, despite several already coming into compliance. Innovation is important to small businesses, especially in rural America. The new European standards have created massive hurdles for these businesses to be in compliance. Many small companies in Europe are already expressing an inability to afford the legal consequences. For example, if a rural grocery store advertises online and provides a link to coupons. Under the GDPR compliance rules, this simple practice can result in expensive legal consequences. For those who do business in Europe, do you think GDPR has the potential to have negative impacts on rural small businesses in Europe?

Answer. Yes. GDPR carries significant compliance requirements for the handling, retention, and deletion of personal data. Amazon is a well-resourced company with exceptional technical talent; however, meeting GDPR's specific requirements caused us to divert significant resources away from our core mission of invention on behalf of customers. Small-and medium-sized businesses are important customers for Amazon, and we remain concerned this regulation can have the effect of hampering small-and medium-sized businesses with less resources.

Question 7. California has already passed a sweeping consumer protection law that threatens established business models throughout the digital sector. I appreciate the industry taking the initiative in creating a framework, in addition to the privacy principles released by the U.S. Chamber of Commerce.

As we begin discussing the appropriate position of the Federal government, can you describe what actions we should investigate more closely for any potential national framework?

Answer. Privacy issues are complex, and there is great risk of unintended consequences from privacy regulation that is not carefully crafted to deliver clear privacy benefits. When answering privacy questions we start with the customer and work backwards. Customers should know how their data is being used and be empowered to make their own individual determination of the benefits they gain from choosing to use new services and technologies. We believe that policymakers and companies like Amazon have very similar goals—protecting consumer trust and promoting new technologies. Congress should contemplate a Federal framework that meets individuals' reasonable expectations with respect to how the personal information they provide companies is collected, used, and shared, and their attendant rights; that includes mechanisms for customers' rights and controls that provide commensurate privacy benefits to customers; that is mindful of the impact of regulation on small-and medium-sized companies; and that applies consistently across all entities and segments of the economy.

Amazon is a member of the Internet Association (IA) and we encourage policymakers to look to the IA's Privacy Principles available at *https://internetassociation.org/positions/privacy/* as they begin to explore a potential national framework.

Question 8. Who, in your opinion, is the appropriate regulator to oversee any framework and why?

Answer. A national privacy framework should primarily be enforced by the Federal Trade Commission (FTC). The FTC is the U.S. regulator with core competency and subject matter expertise on consumer privacy, and should continue to serve that role in future frameworks.

Question 9. According to recent research by Magid, a media research firm, 35 percent of millennials share their password to access streaming services. I certainly understand that the terms and conditions of these services already note that access is for personal use and not to be shared with others. And that the account holder remains responsible for the actions of that third party. However, as the number younger generations sharing their password grows so has the potential for abuse. This "overly sharing of passwords" and the younger generation operate differently than many my age.

Are your policies flexible to cover a third party that may use a friend's or spouse's password? Is this something we should consider as we create Federal guidelines?

Answer. We take account security very seriously and have a number of ways we can identify logins that do not appear to come from the account owner. We do understand that many customers have a legitimate need to share the benefits of our services, so we have designed those services to allow such sharing without needing to share passwords. Prime members can share benefits in their Amazon Household without having to share individual passwords.

Sharing benefits through Amazon Household requires both adults to link their accounts in an Amazon Household and agree to share payment methods. Each adult keeps their personal account while sharing those benefits at no additional cost. Teen logins allow up to four teens (aged 13—17) in the same household to have their own independent Amazon login connected to their parent's account.

Question 10. Thank you Mr. DeVore for meeting with me earlier this week, I wanted to touch on something we discussed in my office. Smart speakers (like Alexa, Google Home, HomePod) have dominated the market place in recent years. They have opened up our homes to A.I. integration allowing us to control our homes, plan out our lives, or purchase things just by asking. However, these always on devices have also raised privacy concerns. It is important to note that always listening is not always recording. Could you briefing go through how my voice is recorded on your devices, stored, and secured?

Answer. Alexa is a cloud-based voice service that lets customers play music, ask questions, make calls, send and receive messages, get information, news, sports scores, weather, and more. Alexa is available through a wide range of products, including Amazon's Echo family of devices, other Amazon products such as our Fire TV and Fire tablet devices, and devices developed by third party manufacturers participating in our Alexa Voice Service program. Alexa operates in a similar manner across the range of products on which it is available, although customers access Alexa differently based on the type of Alexa-enabled product they use.

From early-stage development, we built privacy deeply into the hardware and service by design, and with Alexa and Amazon's Alexa-enabled products we strive to put the control with our customers. On our Echo family of devices, customers speak to Alexa by saying the "wake word" (Alexa, Amazon, Echo, or Computer) or, on some Echo devices, by pressing the action button on the top of the device. Echo devices use "on-device keyword spotting" technology that analyzes acoustic patterns to detect when the wake word has been spoken using a short, on-device buffer that is continuously overwritten. This on-device buffer exists only in temporary memory (RAM); no audio is ever recorded to any on-device storage. The device is effectively always in standby mode, with the wake word functioning as an audible "on switch," and the device does not stream audio to the cloud unless the wake word is detected or the action button is pressed. The user experience also provides customers with a clear indication of when the device is turned on and audio is being streamed for the purpose of processing. When the wake word is detected or the action button is pressed, a visual indicator appears on the device to clearly indicate to the customer that it is streaming audio to the Amazon cloud (*e.g.,* a blue light ring on the Echo device and a blue bar on the Echo Show's screen). We also offer a setting where customers can choose to hear an audible tone when their Echo device begins and ends streaming audio to the cloud.

When audio is streamed to the Amazon cloud, our systems for "automatic speech recognition" (converting audio to text) and "natural language understanding" (interpreting the meaning of text) determine the meaning of the customer's request so that Alexa can respond appropriately. Amazon encrypts all communication between Echo devices and Amazon's servers, and stores all customer data securely on our servers.

We also give customers control of their voice recordings in the cloud. Not only are customers able to see and play back the voice recordings associated with their account, customers can also delete those voice recordings one-by-one or all at once.

Echo devices also come with a "microphone off" button that enables customers to manually control when their device's microphone is on. When the button is pressed to turn the microphones off, the microphones are electrically disconnected and a dedicated red LED is illuminated to indicate the microphones are off. As an additional safeguard, we designed the circuitry of Echo devices so that power can only be provided either to this dedicated red LED or to the device microphones, not to both at the same time. As a result, if the dedicated red LED is illuminated, the microphones are off and cannot stream audio to the cloud.

Customer trust is of the utmost importance to our continued success, and we take that responsibility most seriously.

Question 11. Since I can ask Alexa to order me an Uber, I am curious about what information is shared with third parties to complete a booking or confirm a ride share? (Understanding that I've already given permission to perform these services)

Answer. We design our products and services to limit the amount of personally identifiable information that may be shared, and to share that information in a way that's transparent to our customers. We do not share a customer's personally identifiable information with developers through these products and services without the customer's agreement. We take the privacy and security of our customers' data seriously, and we regularly review our privacy practices and related customer messaging and revise them as appropriate.

For example, when a customer with an Echo device interacts with an Alexa "skill" (Alexa's equivalent of an app) provided by a third party developer, we do not share the customer's identity with the skill developer. Only when a customer chooses to share their identity with a developer—*e.g.,* if a customer takes steps to link their Amazon account to their Uber account so they can request a ride through Alexa—is the developer able to associate usage of the developer's skill with that customer's name. We share with the developer the content of the customer's request to the skill so the skill can respond accordingly, but we only share personally identifiable information to which the customer has granted the developer access. As a result, customers are involved anytime we share their personally identifiable information with a skill developer. Customers can also change these permissions at any time from their Alexa app.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO ANDREW DEVORE

Question 1. GDPR establishes a right of data portability, which some believe is key to driving new innovation and competition within the emerging data ecosystem. Others are concerned that data portability rights, depending on how crafted, could further entrench incumbent companies.

What questions should policymakers be asking in developing data portability rights?

Answer. We encourage policymakers to explore what specific consumer benefit is to be achieved by any new legislation, and how best to accomplish that benefit while avoiding potentially serious downside risks. There are circumstances where portability may be useful to a consumer, and others where it would not serve any useful purpose and may even be counterproductive, including potentially threatening the privacy of other individuals, posing fraud and security risks, and fueling third party markets that trade in personal data.

Question 2. What improvements would you make, if any, to Art. 20 of GDPR, which addresses the right to data portability?

Answer. Consumers that have uploaded personal information into a service should be able to easily download that information so that they can transfer it to another service. But the right of portability should not require that a company produce that information in a proprietary format or in a way that creates security risks or exposes a company's trade secrets or intellectual property.

Question 3. How best can data portability rights be crafted to create new competition, but not further entrench incumbent companies?

Answer. Consumers that have uploaded personal information into a service should be able to easily download that information so that they can transfer it to another service. But the right of portability should not require that a company produce that information in a proprietary format or in a way that creates security risks or exposes a company's trade secrets of intellectual property.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO ANDREW DEVORE

Question 1. When devices get old they get to a point where they cannot support updates for the device the operating system or the many applications run on the device. What is the obligation of the device manufacturer's, operating system programmers, and app developers and programmers regarding to older devices?

Answer. There is no industry-wide practice here and it would be difficult to develop one due to the wide variety of devices, operating systems, and services. Our practice is to provide regular updates (including security updates) to our devices which are automatically applied if the customer is connected to the Internet.

Question 2. What guidelines do your companies follow when it comes to communicating with consumers when either the hardware or software they are using can no longer support updates—especially when these updates relate to security? Is there an industry wide practice that applies here?

Answer. There is no industry-wide practice here and it would be difficult to develop one due to the wide variety of devices, operating systems and services. Our practice is to provide regular updates (including security ones) to our devices which are automatically applied if the customer is connected to the Internet. We also notify customers about important updates on our online support pages when appropriate, and in the past, we have even resorted to postal mail to help notify customers of important updates when their device wasn't connected to the internet. We are obsessed with our customers and constantly thinking about how to build the best possible products for them. Our business model is not built around getting people to constantly upgrade their products. We love that people continue to use our products for many years.

Question 3. What is a reasonable consumer expectation with regard to how long the device will be viable?

Answer. The expected lifetime of a device can vary widely by product, manufacturer, and customer use. Customers should look to the warranty on their device as a starting point, though in many cases products will have a useful life well beyond the length of the warranty period. Our business model isn't built around getting people to constantly upgrade their products.

Question 4. The EU has considered promoting a voluntary labeling system informing consumers about a product's durability, upgradeability and reparability. What do you think of this idea?

Answer. We support the goals of the EU's policy concept; however, details matter. In order to be useful for customers, any such labeling system would need to be online and dynamic to provide up-to-date information and allow manufacturers to continue improving products for their customers even after they are sold.

Question 5. Should devices come with an expiration date in order to manage consumer expectations and more importantly their awareness of their online safety?

Answer. Expiration dates are unlikely to further the goal of promoting improved consumer awareness of online safety. Online safety depends on many factors, including how customers use the products they purchase. An expiration date could give customers a false sense of security and decrease the likelihood that they take important steps to manage their online activity (for example, by avoiding unsecured Wi-Fi networks and regularly updating their apps). Expiration dates could also incentivize manufacturers to promote early device replacements, encouraging customers to update products that may not need to be replaced to maintain robust security.

Question 6. In general we have been exploring the idea of opt in frameworks to keep consumers informed about what their data is being used for. However, we know from recent history that there are some uses of data that should never be permitted—like the leveraging personal data to interfere with election processes. How could we design an opt in framework that is meaningful to consumers, doesn't desensitize them to important decisions about privacy and makes sure they consent only to lawful uses of their data?

Answer. We do not think it is a question of opt-in or opt-out. What is appropriate in any given circumstance is driven by customer expectations based on context. Customers want a friction-less experience and we strive to tie data collection to a concrete benefit that is intuitive and transparent, like our product recommendations.

Question 7. Short of regulation, what more can you and your colleagues and competitors do to restore and maintain our and our constituents' trust that you won't continue to collect more data than consumer understand, use it in ways they never imagined, and then fail to protect the data from unauthorized use and access?

Answer. Earning and keeping our customer trust is the guiding star of our business. We know people will not want to do business with us if they can't trust us to handle their information carefully and sensibly. Consumers have more choice than ever in retail, and we never want our customers to be surprised by what types of data we collect and how we use it. That's why we've built conspicuous signals, notice, and controls into our products and services.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO ANDREW DEVORE

Question 1. State Preemption: Several public interest organizations have written the Committee in advance of the hearing expressing their deep concerns about state preemption. As the ACLU noted, it has often been the states—not the Federal Government—that have acted in a timely and important way to protect consumer interests.

Please provide to me a set of recommendations for how to improve the California Consumer Privacy Act and the GDPR.

Answer. Amazon supports the CCPA's goals of giving consumers visibility and control when businesses collect and sell their personal information. However, because the CCPA was quickly enacted there was little opportunity for thoughtful review, resulting in some provisions that ultimately do not promote best practices in privacy. For example, while the GDPR explicitly encourages the use of pseudonymization of data as a well-known and broadly accepted privacy enhancing practice, the CCPA's broad definition of personal information actually discourages such a practice. Additionally, the CCPA's definition of sale of personal information is so expansive that it not only covers the practices of data brokers who actually sell personal information, but could also inadvertently regulate the basic functions of the Internet such as website analytics that require IP addresses exchanged without any tie to a customer's identity. We also recommend improving the CCPA by providing the California Attorney General the exclusive authority to enforce any violations of the law. Unless the CCPA is substantially improved, we do not consider it a reasonable framework that should be emulated on the national level.

Our long-standing commitment to privacy aligned us well with the GDPR principles, and we did not need to make substantial changes to our customer experience in order to come into compliance. However, meeting GDPR's specific requirements for the handling, retention, and deletion of personal data required us to divert significant resources to administrative and record-keeping tasks and away from inventing new features for customers and our core mission of providing better service, more selection, and lower prices. We encourage Congress to consider the process demands upon business that any legislation might require and the extent to which they actually increase consumer privacy.

Question 2. Privacy by Design: Between the six of your companies, you have access to an overwhelming amount private information about nearly everyone in the United States. AT&T and Charter have access to the browsing history of your customers. A Princeton study found that Google collects visitor data from 70 percent of websites—including from Twitter, a competitor. It's hard to imagine what your companies don't know.

Would you commit to privacy-by-design—limiting collection of data and deleting data when it is no longer useful to your customers?

Answer. Our customer-centric approach has led Amazon to follow privacy by design principles since our founding and we practice the principle of data minimization. Our customers know that their personal information is safe with us, and we know that we must get privacy right in order to meet our customers' high expectations. We use our customer data to innovate and improve the customer experience, and we focus on privacy at all stages of product development through privacy-by-design principles and through robust controls and practices. If anonymous or de-identified data would have comparable utility, we strive to collect the data in that way. And, where appropriate, we provide customers with tools to limit collection, or delete their data. For example, we give customers control of their Alexa voice recordings in the cloud. Not only are customers able to see and play back the voice recordings associated with their account, customers can also delete those voice recordings one-by-one or all at once.

Question 3. What specific steps do you plan to take to limit your own use of customer data? Can you provide examples where you deleted or stopped collecting data to protect privacy?

Answer. Amazon practices the principle of data minimization. Our customers know that their personal information is safe with us, and we know that we must

get privacy right in order to meet our customers' high expectations. We use our customer data to innovate and improve the customer experience, and we focus on privacy at all stages of product development through privacy-by-design principles and through robust controls and practices. If anonymous or de-identified data would have comparable utility, we strive to collect the data in that way. And, where appropriate, we provide customers with tools to limit collection, or delete their data. For example, we give customers control of their Alexa voice recordings in the cloud. Not only are customers able to see and play back the voice recordings associated with their account, customers can also delete those voice recordings one-by-one or all at once.

Question 4. Privacy by design is fundamental to the GDPR. What specific changes have you made to your products to come into compliance to the GDPR's privacy-by-design requirements?

Answer. Our long-standing commitment to privacy aligned us well with the GDPR principles. We had to make little to no changes to our products in order to come into compliance with GDPR. However, meeting GDPR's specific requirements for the handling, retention, and deletion of personal data required us to divert significant resources to administrative and record-keeping tasks and away from inventing new features for customers and our core mission of providing better service, more selection, and lower prices.

Question 5. FTC Rulemaking: In most of your remarks, you discuss the challenges of regulating evolving technologies and economies. It would seem to me that this requires a Federal agency that is responsive to technology changes.

Would you support the FTC having rulemaking authority to provide clarity, to address potential harms, and to ensure rules match technology changes? What sorts of areas should this cover?

Answer. The FTC has demonstrated a vigorous approach to enforcement activity that achieves both immediate and longer-term goals, by stopping inappropriate handling of consumer data; requiring companies to commit to long-term plans that are designed to ensure data handling will be legally compliant in the future; and providing guidance on achieving regulatory compliance in areas where existing standards may be unclear.

The FTC may need new resources to deal with any new consumer privacy framework. In addition, the FTC has always embraced a mission of educating consumers on their rights and protections under the law, and this effort should be encouraged and appropriately resourced. Rulemaking authority may be appropriate in certain instances; however, the record should be fully developed, and show a compelling need before reaching any conclusions regarding expanded authority.

Question 6. AWS Infrastructure in China: During the hearing, Senator Gardner asked with respect to Amazon whether a Chinese subsidiary has access to data Amazon previously stored and maintained on those assets on in China? Mr. DeVore answered with respect to "control" rather than access.

Are Amazon employees capable of accessing the data stored within instances on the Elastic Compute Cloud platform without the consent of the customer?

Answer. First, AWS customers own and control their data at all times. Second, we are vigilant about our customers' privacy and have implemented sophisticated technical and physical measures to prevent unauthorized access. We have a world-class team of security experts monitoring our systems 24/7 to protect customer content. We will not disclose customer content in response to requests unless required to do so to comply with a legally valid and binding order, such as a subpoena or a court order. Additionally, when possible we would notify the customer before disclosing their content so they could seek protection from disclosure. It's also important to point out that customers can choose to encrypt their content as part of a standard security process for highly sensitive content. AWS provides tools customers can use to encrypt their data at rest or in motion, or customers can choose from a number of supported third party security solutions. Content that has been encrypted is rendered useless without the applicable decryption keys.

Because AWS customers retain ownership and control of their content, they can choose which location to store and process their content, and AWS does not move the content unless directed by the customer. This means that if a customer chooses to store and process their content in one of our EU Regions, in Ireland, Frankfurt, or London, it will stay in the EU, in the region they choose. Customers that work with personally identifiable information, or commercially sensitive content, are confident in their choice of AWS as this helps them to comply with EU data protection laws.

Question 7. Have employees of Beijing Sinnet Technology Co. Ltd. or any other third party been provided this level of access to Elastic Compute Cloud instances?

Answer. No.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO ANDREW DEVORE

Question 1. Unsurprisingly, none of your testimony speaks about potential increased penalties for a new privacy framework. The current penalty regime seems not to change corporate behavior—as we repeatedly have seen. In your opinion, are civil penalties an effective mechanism to push companies to follow the law? If not, what mechanisms would be effective?

Answer. Civil penalties in the right context and case can be an effective tool for an enforcement body. In most cases, however, it is likely better for consumers to have any specific actual harm remedied.

Question 2. Since both Apple and Amazon's inception, 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 with Alexa and Siri. As both Apple and Amazon were creating this next generation of interfaces, what specific measures did each of your companies take to ensure that these new technologies complied with COPPA?

Answer. Children's privacy is important to Amazon. Our Children's Privacy Disclosure (*https://www.amazon.com/gp/help/customer/display.html?nodeId=202185560*) and the Amazon Privacy Notice (*https://www.amazon.com/gp/help/customer/display.html?nodeId=202185560*) describe how we handle personal information we collect from children under the age of 13.

Consistent with the Children's Online Privacy Protection Act, we require verifiable parental consent before child directed services like FreeTime on Alexa can be used. Unless a parent has granted permission previously, the first time the parent attempts to set up FreeTime on Alexa, the parent will be prompted to provide verifiable parental consent on the Alexa app through either credit card verification or a one-time code sent via SMS. Parents can review or change permissions by visiting the Manage Parental Consent page on Amazon.com (Manage Parental Consent) or by contacting Customer Service (*https://www.amazon.com/contact-us*). Parents can also contact Customer Service (*https://www.amazon.com/contact-us*) to request deletion of any personal information collected through FreeTime on Alexa. We do not share kids' voice recordings with any third party.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO ANDREW DEVORE

Question 1. Positive Aspects of State Laws/GDPR: Your company has called for a national privacy framework in order to avoid a patchwork of state laws which you have to comply with as your data travels across state lines. From an international perspective, Europe has GDPR. You have operations around the country, and some around the globe and have seen firsthand how these laws are being implemented.

Are there any states that you believe have the right framework, or aspects, in place?

Answer. We have been encouraged by laws in several states. Nevada requires companies to provide notice to consumers of their practices relating to the collection and disclosure of personal information. Washington State enacted a biometric privacy law in 2017 that imposes reasonable limitations on the sale and disclosure of biometric information. However, we do not believe that privacy should be regulated on a state-by-state basis, and urge Congress to develop a national approach.

Question 2. Can you point to an aspect of the California law that you believe is reasonable and should be emulated on the national level?

Answer. Amazon supports the CCPA's goals of giving consumers visibility and control when businesses collect and sell their personal information. However, because the CCPA was quickly enacted there was little opportunity for thoughtful review, resulting in some provisions that ultimately do not promote best practices in privacy. Unless the CCPA is substantially improved, we do not consider it a reasonable framework that should be emulated on the national level.

Question 3. Nevada passed a privacy notice law during the 2017 session, how is your company doing in complying with this?

Answer. We clearly communicate our policies and practices in our terms of service and privacy notice, consistent with the requirements of Nevada's law.

Question 4. What part(s) of the GDPR should we look to emulate in the U.S?

Answer. Several core features of the GDPR are instructive as policymakers contemplate a national framework. First, the requirement that businesses that collect the personal data of consumers transparently disclose to the consumer what data they collect, how they use it, and whether and when they transfer the personal data to third parties. Second, the consumer's right to access, upon request, their personal data that a business has in its possession, subject to the business's right to withhold data for security and anti-fraud reasons. Lastly, the consumers' right to request deletion of their data, subject to a business's right to retain data in furtherance of its legal obligations and rights and for security and anti-fraud purposes.

Question 5. State Attorneys General: I understand the utility of having a national framework given how difficult it would be to develop 50 different frameworks based on state law. At the same time, we want to ensure that states play a role in protecting the privacy of their residents.

What should, in your view, be the role of State AGs in enforcing privacy standards?

Answer. State Attorneys General play an important role in consumer protection and enforcing the law. Should the Federal Trade Commission (FTC) choose not to act on a matter, it would be appropriate for a state's Attorney General to use their authority.

Question 6. Law Enforcement: I believe our law enforcement officials should have a mechanism to obtain the data they need for legitimate investigations. At the same time we need to strike the right balance between keeping our country and communities safe while protecting individuals' civil rights and privacy. Your company has access to many of the personal and intimate choices of millions of your customers, data and records that paint the picture of the everyday lives of millions of American families.

How do you believe a national privacy framework could seek to strike the right balance?

Answer. Customer privacy is paramount to Amazon and we remain committed to advocating for legislation and policies that protect customers from unlawful access to electronic data. Amazon will only share customer information in response to valid court orders, subpoenas, or other legally binding requests. We have and will continue to challenge government subpoenas for customer information if we believe them to be over-broad. We will also continue to work with Federal and state legislatures to modernize outdated laws to enhance the privacy and security of our customers' data by preventing law enforcement from accessing content without a warrant. We welcome the opportunity to work with Congress to ensure that law enforcement agencies are provided with clear legal frameworks that require valid legal process for customer data. We oppose legislation mandating or prohibiting security or encryption technologies that would have the effect of weakening the security of products, systems, or services our customers use, whether they be individual consumers or business customers.

Question 7. Privacy Enhancing Technology: There are many technologies that actually enhance users' privacy: Encryption, anti-virus, cybersecurity technologies are all examples of this. I think this is a portion of the privacy debate that sometimes gets looked over, but one we should consider as we look at privacy legislation.

Can you summarize some of the privacy enhancing technology used at your company?

Answer. We are vigilant about our customers' privacy and have implemented sophisticated technical and physical measures to prevent unauthorized access to data. A team of highly qualified security experts monitors customers' data on a 24/7 basis and secures their privacy. We have research and scientific teams across the company dedicated to innovating both technology and privacy-aware techniques to assist our product development teams in privacy-by-design. Although many of these privacy enhancing techniques include confidential, proprietary technology, many of our commonly used techniques include encryption, deidentification, and pseudonymization.

Question 8. Do you believe the Federal Government could assist in either funding the development of similar technologies or establishing a framework for companies to implement them into their data processing?

Answer. The U.S. Government has long been the global leader in innovation policy and research and development. Thoughtful policymaking that puts the consumer first will lead to continued innovation in privacy protective products and features. Privacy frameworks should ensure that any additional overhead and administrative demands placed on organizations do not displace research and development in privacy enhancing technologies. Likewise, we encourage the U.S. Government to make funding for long-term research initiatives a priority. Much of the success in private

sector technology today is built on years of research under the United States' stewardship.

Question 9. Small Business: As we talk about a national framework, one of the most important things to keep in mind is how we work with small business. Your company has the ability to maintain cybersecurity and compliance teams that make it easier for your companies to work with any potential law we pass.

Can you discuss how your companies might be working with, or aiding, small businesses with their privacy and data needs?

Answer. Amazon Web Services (AWS), our cloud services business, is committed to offering services and resources to our customers—including small businesses—to help them comply with privacy requirements that may apply to their activities. AWS regularly achieves third party validation for thousands of global compliance requirements that we continually monitor to help customers meet security and compliance standards for finance, retail, healthcare, government, and beyond. Our customers benefit substantially from the many security controls operated by AWS, strengthening their own compliance and certification programs, while at the same time providing tools to reduce the cost and time of running their specific security assurance requirements. These security and privacy benefits are particularly valuable for small businesses that would have difficulty building such protections and controls themselves.

Question 10. Also, can you provide your thoughts on how a Federal framework would best take the challenges and opportunities of small businesses into account?

Answer. Data privacy is a complex issue with potentially far ranging effects, so the details are critical. In crafting privacy proposals, Congress should carefully consider each detail and the potential unintended consequences on users and the economy, particularly small-and medium-sized businesses. Overly prescriptive requirements for the handling, retention, and deletion of personal data would place great demand on any systems or business team. We encourage Congress to consider the process demands upon business that any legislation might require and the extent to which they actually increase consumer privacy. We also encourage Congress to create a single Federal solution that will relieve SMBs of the burden of trying to comply with a patchwork of state laws, as those businesses are least equipped to meet such conflicting demands.

Amazon is a member of the Internet Association (IA) and we encourage policymakers to look to the IA's Privacy Principles available at *https://internetassociation.org/positions/privacy/* as they begin to explore a potential national framework.

Question 11. Data Protection Officers: As you all 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 company's perspective on this requirement?

Answer. We comply with the GDPR, but we do not believe a one size fits all approach is right for customers or innovation. At Amazon, we embed privacy experts and lawyers into each product team to ensure every customer product, service, and feature has direct privacy expertise, stewardship, and compliance. These experts have the authority to act as their business's "DPO," meaning every product and service receives the direct privacy attention it deserves. This is good for customers and our business.

Question 12. Data Minimization: One component of the GDPR is a concept known as "data minimization." This principle states that data processing should only use as much data as is required to successfully accomplish a given task and data collected for one purpose cannot be repurposed without further consent. The idea behind this is both to ensure that users are comfortable that their data is only being used for the purposes which enhance the experience and also help limit the impact of any data breaches.

It seems like there may be challenges to implementing something this broad, especially as it is laid out in the GDPR, but it nonetheless feels like something that should be explored as part of our conversation here in the United States.

What is your company's perspective on this requirement?

Answer. Amazon practices the principle of data minimization. Our customers know that their personal information is safe with us, and we know that we must get privacy right in order to meet our customers' high expectations. We use our customer data to innovate and improve the customer experience, and we focus on privacy at all stages of product development through privacy-by-design principles and through robust controls and practices. If anonymous or de-identified data would

have comparable utility, we strive to collect the data in that way. And, where appropriate, we provide customers with tools to limit collection or delete their data. For example, we give customers control of their Alexa voice recordings in the cloud. Not only are customers able to see and play back the voice recordings associated with their account, customers can also delete those voice recordings one-by-one or all at once.

Question 13. 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.

Do you build your own data centers or contract with another entity?

Answer. We carefully manage every aspect of data center construction, with a foundational focus on physical and cyber security.

Question 14. What steps do you take to secure these centers?

Answer. We have an elaborate and state-of-the-art approach to both physical and logical security covering our systems, processes, and people. These measures are regularly and frequently tested by us, and also audited by a variety of third party auditors under various audit and compliance regimes. Such third party validation is just one way to demonstrate to our customers and APN Partners that we are protecting the personal data they choose to process on AWS. AWS has achieved a number of internationally recognized certifications and accreditations, demonstrating compliance with third party assurance frameworks, such as ISO 27017 for cloud security, ISO 27018 for cloud privacy, and SOC 1, SOC 2 and SOC 3. Customers can be PCI and HIPAA compliant on AWS, and we have achieved important certifications like FedRAMP and SRG Impact Levels 2, 4, and 5 for DoD systems. These certifications help support customer compliance with requirements such as ITAR, FISMA, CJIS, and NIST 800–53 and 171. We also have ISO9001 which is primarily for healthcare, life sciences, medical devices, automotive and aerospace.

Security will always be our top priority. Examining the AWS cloud, you'll see that the same security isolations are employed as would be found in a traditional data center. These include physical data center security, separation of the network, isolation of the server hardware, and isolation of storage.

Amazon and AWS are vigilant about our customers' privacy and have implemented sophisticated technical and physical measures to prevent unauthorized access. We have a world-class team of security experts monitoring our systems 24/7 to protect customer content. It's also important to point out that customers can choose to encrypt their content as part of a standard security process for highly sensitive content. AWS provides tools customers can use to encrypt their data at rest or in motion, or customers can choose from a number of supported third party security solutions. Content that has been encrypted is rendered useless without the applicable decryption keys.

See *https://aws.amazon.com/compliance/data-center/data-centers/* and more generally *https://aws.amazon.com/compliance/* for more information.

Question 15. How often to you review your physical data security standards at your data centers?

Answer. Frequently and regularly, both with internal and external testing and auditing, see above.

Question 16. Drone Privacy: Most of what is being discussed in user interaction with platforms and how those platforms use their data. Amazon is working heavily with unmanned aerial systems (UAS), or drones. With technology like this, data could potentially be collected without any user involvement at all.

For example, a drone could, while delivering a package, take notice of another item sitting on your front porch or collect data on what types of things your neighbor has purchased in their front yard.

How do we capture these types of contingencies in a data privacy law?

Answer. We're excited about Prime Air—a future delivery system from Amazon designed to safely get packages to customers in 30 minutes or less using unmanned aerial vehicles, or drones. Prime Air has the potential to enhance the services we already provide to millions of customers through the introduction of rapid parcel delivery that serves customers and safely improves the efficiency of our transportation system, but this begins with customer trust. We use information in a responsible, appropriate, and secure manner to innovate and improve the customer experience, and we know we must get privacy right to meet our customers' high expectations of us. We recognize that drone technology must be incorporated in a sensible, pri-

vacy-conscious manner, which is why we endorsed the National Telecommunications and Information Administration (NTIA's) voluntary best practices for drone privacy, transparency, and accountability. *https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf*

Question 17. Will Amazon use drones for this purpose, even if it takes place in the course of package delivery or other specific priority purposes?

Answer. No, Amazon Prime Air, our future delivery system for package delivery via drones, will not be a surveillance service. Any data collected by our drones will be used to improve the performance, safety, and reliability of our systems.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO KEITH ENRIGHT

Question 1. Google is subject to an FTC order issued in 2011 that, among other things, required Google to establish and implement, and thereafter maintain, a privacy program designed to: "(1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information." In 2012, Google paid a $22.5 million civil penalty to settle allegations that it violated the FTC order. Please describe the steps Google has taken to comply with the FTC's order.

Answer. We are committed to ensuring compliance with our FTC consent decree and have dedicated significant attention and resources to ensuring the commitments we made to the FTC are met. Our comprehensive compliance program—one of the most sophisticated in the world—includes:

- Yearly risk assessments, strong internal policies that guide our employees, and training and advice by our privacy and security experts to ensure compliance with our FTC Consent decree and the protection of our users.
- Compliance checks and controls. Product launches and changes to existing products are gated by a unified privacy and security review process ensuring the product's data lifecycle, covering data collection, use, notice and control, sharing, storage and access, and deletion and retention.
- Strong incident response procedures. Potential privacy issues are addressed through our robust incident response program for privacy- and security-related events. Employees are required to report any suspected security or privacy incidents to our dedicated 24x7x365 worldwide incident response teams, so that we can respond, including by securing and protecting users' data and handling user notifications.
- Regular external assessments—three separate, globally recognized external assessors assess our program on a bi-annual basis. They each have found that our program was operating effectively.

But we will not stop there. We are always looking for ways to refine and improve our privacy program and continue to focus that effort.

Question 2. What, if any, additional steps did Google take to comply with the FTC order after agreeing to settle allegations that it violated the order in 2012?

Answer. In this instance, Google moved swiftly to correct an inaccurate statement on our Help Center and to fix an issue with cookies being set where we did not intend as a result of changes made in third-party software. We also took steps to ensure this type of issue could not arise in the future. This work and our agreement with the FTC resolved the matter and allowed us to move on to launching great, privacy-protective products and features.

Question 3. On July 22, 2018, Google responded to questions posed by me, Telecommunications Subcommittee Chairman Wicker, and Consumer Protection Subcommittee Chairman Moran in a letter dated July 10, 2018, regarding the use of Gmail users' personal data by third party e-mail app developers. I have some follow-up questions based on Google's response, which did not fully answer all of the questions we posed in July.

Google said that it pre-installs "Google Play Protect" on all Google-licensed Android devices to continuously monitor users' phones, along with apps in Play and across the Android ecosystem, for potentially malicious apps. Google also asserted that it scans more than 50 billion apps every day and warns users to remove apps Google identifies as malicious.

a. Does Google take any steps to protect consumers from the potentially malicious apps it has identified, other than warning consumers about them? If so, what are these steps?

Answer. Yes, Google Play Protect includes on-device capabilities that protect users from potentially harmful apps in real-time, as well as services that analyze device and app data to identify possible security concerns. In 2016, we started scanning all devices for potentially harmful applications once a day. Daily scanning allows Google Play Protect to respond quickly to a detected threat, reducing how long users could be exposed to the threat and how many devices may be affected. Google Play Protect leverages cloud-based app-verification services to determine if apps are potentially harmful. If it finds a potentially harmful application, Google Play Protect warns the user. In cases of severe malware, Google Play Protect can remove the potentially harmful application from affected devices and block future installs. This furthers user safety and mitigates the potential harm the app can cause while providing minimal inconvenience to the user and providing them with control over their device.

Question 4. How many potentially malicious apps has Google identified over the last year? How many consumers heeded Google's warning and removed these apps? Did Google follow up with consumers who did not remove these apps? If so, how?

Answer. In 2017, daily Google Play Protect scans led to faster identification and removal of approximately 39 million potentially harmful applications. We automatically disabled such applications from roughly 1 million devices. In November 2017, we updated Google Play Protect to disable potentially harmful applications without uninstalling them. When we can, we try to leave as much choice in users' hands as possible. To walk the line between user choice and safety, when Google Play Protect detects certain kinds of potentially harmful applications, it automatically disables the app. Users are asked to uninstall the app or re-enable it without losing their data. This mitigates the potential harm the app could cause while providing minimal inconvenience to the user while they decide what to do. If the user decides to not respond to a Google Play Protect warning, detected harmful apps that remain on the device will always be presented to the user on the main Play Protect settings screen, so they can get back to this later if they want.

Question 5. In its July 22, 2018, response Google said it acts promptly on user reports about privacy and security issues, rewards researchers and developers who flag privacy and security issues, and engages in research and community outreach on privacy and security issues to make the Internet safer.

a. What specific steps does Google take in response to user reports about privacy and security issues?

Answer. Whenever a user reports a potential privacy or security issue, the appropriate team promptly investigates the circumstances surrounding the report to determine whether further action is warranted. The action taken depends on the result of that investigation. For example, if a user reports an app's potential violation of the Play Store's policies, and our review confirms the violation, the relevant app may be removed from the Play Store. As another example, a user report about a security bug in a third-party app may lead us to contact the relevant developer and suspend the app until the bug is fixed.

Question 6. How many such reports has Google received during the last year? How many of these reports warranted action by Google, and what action did Google take? How long did it take, on average, for Google to act on these reports?

Answer. Google incentivizes researchers to identify and report vulnerabilities in Google's products and apps as well as in apps developed by partners under various vulnerability reward programs. See *https://www.google.com/about/appsecurity/* for more information. We unfortunately do not have information we can share about the average response time, but we can share that we receive thousands of such leads every year and pay out millions of dollars to researchers for their submissions.

Question 7. How does Google reward researchers and developers who flag privacy and security issues?

Answer. Google has a close relationship with the security research community, and has maintained a Vulnerability Reward Program (VRP) for Google-owned web properties since 2010. Through its VRP, Google encourages researchers to promptly submit reports about any design or implementation issue that substantially affects the confidentiality or integrity of user data. After the bug is confirmed and remediated, a panel of Google's security team reviews and considers the impact of the reported issue and chooses a reward accordingly. Rewards for qualifying bugs can exceed $30,000. In our latest VRP annual report from February 2018, we noted that the program had paid out nearly $12M in rewards to date.

Question 8. How does Google engage in research and community outreach on these issues?

Answer. In addition to the VRP described above, Google maintains a permanent privacy and security research team that is dedicated full time to researching privacy

and security issues. This research serves both to inform the teams building products about important privacy and security issues, as well as to engage and contribute to the vibrant research community, and is frequently published and presented in external journals and conferences. These teams also engage directly with users through user experience studies, to ensure that our products and policies are built with users in mind and based on their feedback.

Question 9. In July, we asked Google to provide a list of all instances in which Google has suspended an app for failing to comply with Google's policies, with an explanation of the circumstances for each. Google's written response to our letter did not provide this information.

a. How many apps did Google find to have violated its policies over the last two years? Please provide a list of these apps and describe the nature of the violation found by Google.

b. How many apps has Google suspended over the last two years? How many of these apps were suspended for violating Google's policies?

c. How many apps have been denied access by Google over the last two years? How many of these apps were denied access for violating Google's policies?

d. How many apps did Google provide warnings about over the last two years? How many of these apps violated Google's policies?

e. Did Google subsequently "un-suspend" or restore access to any of these apps? If so, why? Please identify any such apps and explain the circumstances.

We answer questions 9.a through 9.e together.

Answer. In 2017, Google took down over 700,000 apps that violated Google Play policies. This was an approximately 70 percent increase over the number of apps taken down in 2016. This increase was possible due to significant improvements in our ability to detect potential abuse—such as impersonation, inappropriate content, or malware—through new machine learning techniques.

Our agreements with developers outline a range of actions we may take in the event of policy violations, depending on the severity of the violation. For example, we may disable the relevant app or remove it from user devices where it could cause serious harm to the user's device or data; reject, remove, suspend, or demote applications on the Play Store; or ban developers from the Play Store completely. When a developer engages in repeated or serious violations of our policies, such as developing malware or other apps that may cause user or device harm, we terminate their accounts. For example, we employ signals like app similarity and other details about developers to detect such repeat abuse. We've also developed detection models and techniques that can identify repeat offenders and abusive developers at scale. This resulted in suspending and removing the apps of 100,000 bad developers in 2017, and made it more difficult for malicious actors to create new accounts and attempt to publish more bad apps.

Google also works with the developers of apps that are not malicious but nevertheless do not meet our standards, to ensure that they improve and clarify their practices for our users. If those developers accept our recommendations, the app may ultimately be approved.

While the number of apps that are suspended for violations of our policies makes it impossible to describe the individual circumstances underlying each, we provide illustrative examples below to demonstrate how these processes work as safeguards against apps that violate our policies and to protect our users:

1. An app that helped users track another person, in violation of our Malicious Behavior policy (*https://play.google.com/about/privacy-security-deception/malicious-behavior/*).
2. A game that collected personal information but lacked a privacy policy, in violation of our Personal and Sensitive Information policy (*https://play.google.com/about/privacy-security-deception/personal-sensitive/*)
3. An app that collected location data from users in an unsanctioned manner, in violation of our Device and Network Abuse policy (*https://play.google.com/about/privacy-security-deception/device-network-abuse/*)

In addition to the protection provided by Google Play, Google Play Protect provides another layer of security against malware that finds its way on the device, whether it was downloaded from Play or side loaded. As outlined in our responses to question 3(b), Google Play Protect identified and removed approximately 39 million potentially abusive apps in 2017.

Question 10. Google asserted that it tightly restricts its own employees' access to the content of users' Gmail accounts, and that Google conducts routine auditing of employee access to user e-mail message contents.

a. What specific steps does Google take to audit employee access to user e-mail message contents?

Answer. Access to e-mail data is restricted by technical measures to a limited number of Google employees performing legitimate business processes, such as performing debugging, responding to law enforcement requests, or reviewing spam reported by users. Additionally, we have a team of security engineers dedicated to detecting any abuse involving user data access. By design, access to e-mail content by a Google employee is logged, analyzed, and subject to automated detection for potentially malicious behavior, such as accessing an account without an appropriate justification. On top of the automated detection, security engineers regularly analyze logs to detect new anomalous access patterns to investigate.

Question 11. Has Google detected any improper employee access to user e-mail message contents? If so, please describe the circumstances and explain any steps taken by Google to address such improper employee access?

Answer. As we described above, our first goal is always to prevent such misuse via technical and policy means, but a small number of employees must have access to fix issues with our systems.

We have strict policies to ensure that our employees sufficiently protect our users' data. While we are not aware of any misuse by an employee in the last five years, to the extent we do identify misuse by an employee, we will take strong action, including termination.

Question 12. Our July letter asked whether Google was aware of any instance of an app developer sharing Gmail user data with a third party for any purpose. Google responded that it allows developers to share data with third parties "so long as they are transparent with the users about how they are using the data."

a. What specific steps does Google take to ensure that app developers do not improperly transfer Gmail user data to third parties?

Answer. We support our policies on third party access to Gmail user data with verification, monitoring, and enforcement. In addition to the measures described in our previous response, Google's proactive review of apps seeking access to user data also include the use of machine learning tools to detect signals indicative of malicious apps. Depending on the results, a developer's history, and user feedback, we identify apps that need additional manual review. This review can include testing their app directly and reviewing their website materials, among other investigative steps.

In addition, we recently announced even stronger privacy controls. These controls include an improved user permission flow that provides a finer-grained ability to choose what data they share, limiting the types of apps that can request access from Gmail users, and imposing new requirements on how developers must treat Gmail data. These policy changes are going into effect on January 9, 2019.

More specifically, beginning in January 2019, we will only allow specific types of applications—such as e-mail clients and productivity tools (the new policy is available at *https://developers.google.com/terms/api-services-user-data-policy#additional-requirements-for-specific-api-scopes*)—to access certain Gmail APIs. When users grant Gmail access to applications that do not require regular direct user interaction (for example, services that provide background reporting or monitoring to users) users will be provided with additional warnings and be required to re-grant access at regular intervals.

We are also continuing work to ensure compliance with our policy that developers should only request access to information they need. During application review, we will be tightening our review for compliance with this existing policy. For example, if an app does not need full or read access and only requires send capability, we require the developer to request narrower permission scopes so the app can only access data needed for its features.

Finally, our new policies include additional, strict limitations on how data may be used. Apps accessing these APIs can only use Gmail data to provide prominent, user-facing features and may not transfer or sell the data for other purposes, such as targeting ads, market research, e-mail campaign tracking, and other purposes unrelated to these features. As an example, with a user's permission, consolidating data from a user's e-mail for their direct benefit, such as expense tracking, is a permitted use case. However, consolidating the expense data for market research that benefits a third party is not permitted. We have also clarified that human review of e-mail data must be strictly limited.

Question 13. Has Google ever suspended an app for improperly transferring Gmail user data to third parties? If so, please provide a list of these apps and describe the nature of the violation found by Google, including any action Google has taken to recover data.

Answer. As one example of how Google enforces its policies, in June 2018, we identified an app in our verification and review process that appeared to imitate another legitimate company. The deceptive app claimed to make sending and receiving e-mails easier. Our review identified that the app had no such apparent functionality.

In addition, the app exhibited numerous suspicious signals. For example, the app's login page simply redirected users to their Gmail page and was otherwise nonfunctional. The app also claimed to have a demonstration page for users that did not actually exist. The app's request for verification was rejected.

Question 13. In the event of a security lapse involving user data, how does Google determine what constitutes a "significant risk of harm" for its users?

Question 14. As you may know, there is ongoing discussion as to whether there should be some disclosure requirement in the event of a security lapse or vulnerability involving user data, even if it does not constitute a breach or create a "significant risk of harm." Does Google believe some form of disclosure, such as public notice or notice to a relevant regulator, would be appropriate, even if there is not a significant risk of consumer harm?

We answer Questions 13 and 14 together.

Answer. Google operates a robust incident response program for privacy and security-related events. Under this program, employees are required to report any suspected security or privacy incidents to our dedicated 24x7x365 worldwide incident response teams, so that we can respond, including by securing and protecting users' data and handling user notifications. Risk of harm to users is an important criterion for determining whether notification is appropriate. We do, for example, consider whether the type of data at issue is particularly sensitive or whether there is evidence of misuse. But we go beyond that and any legal obligations by applying several considerations focused on our users. These include whether we could accurately identify the users to inform, whether there was evidence of misuse, and whether there were any actions a developer or user could take in response.

While notification is often the right response, it is also important to avoid overnotification, which could impair users' ability to recognize and take action upon the most important notifications. We are acutely aware of the importance of the trust our users have in us. That is why we have—and will—continuously examine our approach to user notifications, always with a focus on the user.

Question 15. Google's Framework for Responsible Data Protection Legislation advocates for legislation that would, among other things: (1) require organizations to take responsibility for the use of consumers' personal data (*i.e.,* data that can be linked to a person or personal device), (2) mandate transparency and help consumers be informed, and (3) require organizations to secure consumers' personal data and expeditiously notify individuals of security breaches that create a significant risk of harm.

a. How does Google's decision not to disclose the vulnerability that potentially exposed the personal data (including name, e-mail address, profile photos) of nearly 500,000 Google+ users comply with the principles reflected in the Framework?

Answer. When we become aware of a potential incident, we always review our legal notification obligations and determined whether a notification is required. But we always go further at Google—looking beyond our legal obligations and applying several considerations focused on our users in determining whether to voluntarily provide notice beyond what the law may require. These include whether we could accurately identify the users to inform, whether there was evidence of misuse, and whether there were any actions a developer or user could take in response. Here, with respect to the G+ bug, the answers to each of those considerations was no, and we decided against notification.

- We did not find evidence of misuse or user harm. As discussed above, we undertook a number of steps in an attempt to determine whether the developers who may have accessed non-public profile data because of this bug abused that access in any way.
- We could not accurately identify affected users. As discussed above, we have not been able to identify the set of specifically affected users and therefore do not know how many users were actually affected or who they are.
- There was nothing users or developers could do in response to notification. Finally, we considered whether this was a situation where we would recommend steps to users or developers in response to the notification. Once we patched the bug, there was nothing more that we could identify that could be done to mitigate the consequences of the bug. Indeed, once we fixed the bug, developers would have had no way after the fact to identify which of the data they accessed

may have been non-public at the time they accessed it nor would we be able to confirm any users' claim that their data was always set to private.

Finally, giving notification in these types of situations, without being able to even tell a user they were affected—frustrates users and contributes to breach notification fatigue, where users begin ignoring important warnings because they are overwhelmed but the number of notifications they receive. We balance that risk with our desire for transparency and our desire to ensure the continued long-established trust of our users.

All of these factors weighed against voluntary notification, and so we made a considered decision not to provide one. Given that there was no notification to users we also did not discern a reason to make a separate notification to Congress. With that said, we are always looking to improve and will continue to look at our approach to user notifications, always with a focus on the user.

Question 16. How did Google determine that the potential exposure of nearly 500,000 Google+ users' personal data, including name, e-mail address, date of birth, and profile photos, to outside app developers without their consent did not warrant notification of the affected consumers?

Answer. First, it is important to understand the limited scope of data that was at issue. The bug allowed apps to potentially access nonpublic profile information that had been shared with a user by another G+ user.

This data was limited to profile fields including name, profile photo, occupation, and gender. (The full list of G+ Profile fields that could be fetched by the relevant API is documented on our developer site at *https://developers.google.com/+/web/api/rest/latest/people.*) It is important to note, however, that many of these profile fields are or may be set to public, and therefore may not have been implicated by the G+ bug at all. Additionally, the fields of data potentially at issue did not include data like Google+ posts, messages, Google account data or G Suite content, nor did it include information about a person's home address, phone numbers, or other types of data typically used for identity theft.

As described above, whenever we become aware of a potential incident, we review our legal obligations. In the course of this review we are reminded of the standards that legislators and regulators around the world have deliberately chosen to implement after having carefully weighed the potential benefits and harms to users of notice following incidents with certain features. If we are legally obliged to give notice, we do so. But we always go further than that—looking beyond our legal obligations and applying several considerations focused on our users in determining whether to voluntarily provide notice even under circumstances where doing so is not legally required.

Those include whether we could accurately identify the users to inform, whether there was evidence of misuse, and whether there were any actions a developer or user could take in response. Here, the answer to each of those considerations was no, and we decided against notification.

Question 17. In its October 8, 2018 blog post about this issue, Google stated that it found no evidence that any of the potentially exposed consumer data was misused. What level of confidence does Google have in this assessment? Does Google have a way to verify that none of the affected consumers' data was impermissibly accessed?

Answer. While we had limited data to analyze, based on what we did review, we are confident that the misuse of this data was highly unlikely.

We undertook a number of steps in an attempt to determine whether the developers who may have accessed non-public profile data because of this bug abused that access in any way.

- First, we surveyed our access logs to identify whether the developers appeared to be making API calls that appeared unusual, for example large volumes of calls. We saw no evidence of an unusually large volume of calls from an app, which, had it occurred, may have suggested that the developer knew it was accessing nonpublic data and was taking advantage of that.
- Second, we took a harder look at the top developers accessing the API to determine whether there was any reason to believe they were not calling the API for a legitimate purpose, or likely misusing the data in some way. The vast majority were apps created by well-known and reputable companies or apps that had already undergone vetting by our teams to be allowed to participate in other developer programs.
- Third, we reviewed individual apps to determine whether their use of the API seemed appropriate given their apps' functionality. The apps were generally the type of apps that would have a legitimate purpose to use the API, *e.g.,* apps

that connect users with their friends, manage their social media profiles, or connect individuals through enterprise apps designed to connect employees within others in their organisation.

- Finally, we have also undertaken a review to determine whether there was any reason to believe the developers were engaged in misuse or deception (for example, whether those apps were known to us to be subject to regulatory inquiries or were otherwise publicly identified as misusing user data). We found no reason to be concerned.

Question 18. Has Google received any complaints from affected consumers surrounding its decision not to notify them of this potential exposure of their personal information?

Answer. We are committed to addressing user concerns on all privacy and security topics, including this one. We are both proactively and reactively reaching out to users to help them understand the G+ bug, and have yet to identify a specific case of user harm.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO KEITH ENRIGHT

Question 1. 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. Your testimony indicated that Google supports the idea of "data portability," and even enables consumer data export from its variety of products. Could you please explain what compliance and enforcement with this GDPR provision looks like? Please describe the consumer benefit of this requirement.

Answer. Google strongly supports the notion that users should be able to export the personal information they have provided to an organization, in a format that allows them to understand the information, store a local copy, and/or to import it into another provider's systems. This has two important consumer benefits. First, it empowers individuals to understand and control their personal information. It also keeps the market innovative, competitive, and open to new entrants by allowing users to easily move to new services without losing the benefit of their accumulated data.

The GDPR is only now entering the earliest stages of enforcement, and we cannot tell precisely how this provision will be interpreted and enforced, but we believe our program meets or exceeds the law's requirements.

More generally, we have worked on portability for over a decade and were the first to offer a portability tool in 2011. We updated and broadened this tool, Download Your Data, last spring so that it now covers more products and data types. The tool allows users to take personal information about them stored in more than 50 Google products, including search queries, Gmail messages and contacts, YouTube videos, and many others. The output is provided in formats designed to be importable into software on the user's own devices or other services.

The ability for users to transfer data directly from one provider to another, without downloading and re-uploading it, is a significant advancement in making portability practical for users all over the world. We are working with partner companies on the Data Transfer Project (https://datatransferproject.dev/), an open-source initiative to expand this capability and make it even easier for users to try a new service or otherwise control their data. The current partners (Google, Microsoft, Twitter, and Facebook) are working on building a user interface as well as bringing new and more diverse partners into the project.

Question 2. 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. Our proposed privacy framework suggests applying general principles in ways that reflect the different resources of different organizations. The overall touchpoints should be accountability and preventing harm, rather than inflexible one-size-fits all rules. Accordingly, we urge the Committee to explore ways to develop the data portability principle to work for businesses of all types and sizes.

One way to further this goal is for industry organizations and government entities like the Federal Trade Commission to explore best practices and methodologies that can be adopted by smaller players—perhaps via open-source projects or other low-cost options. We are working on this already: we recently launched the Data Transfer Project with several industry partners. As we described above, it's an open-

source project that provides tools for any company, big or small, to build direct service-to-service data portability.

Question 3. Efforts to draft meaningful Federal legislation on consumer data privacy will heavily rely upon determinations of what types of personally identifiable data are classified as "sensitive" and what are not. While some have suggested that expanded FTC rulemaking authority is necessary to flexibly account for new types of data sets coming from innovative technologies, I have concerns that excessive rulemaking authority could lead to frequent reclassifications of the types of data with ensuing liability adjustments. Do you have suggestions on how to best identify "sensitive" personally identifiable information?

Answer. This concern is valid, and should be considered when drafting regulatory proposals. Our regulatory framework suggests that "sensitivity" of personal information should be tied in law to risk of harm to individuals and communities, rather than a specific list of data types that might quickly become out of date. We think this is the right approach, but does require thought to avoid unnecessarily shifting regulatory standards.

One possibility is to ensure that regulatory authority over this issue is closely bound to an articulation of risk of harm. While regulators may have the ability via rulemaking or other process to define certain data types that meet this criteria, they must tie such rules to findings that those data types present such a risk of harm.

Question 4. NTIA issued a request for comment on ways to advance consumer privacy without harming prosperity and innovation. I commend the administration for their attention to this important issue. The "High Level Goals for Federal Action" that NTIA is seeking comments for includes interoperability and the development of a regulatory landscape that is consistent with the international norms and frameworks in which the U.S. participates. How do you foresee Federal legislation affecting cross-border data flows?

Answer. A comprehensive Federal data protection law would help promote and sustain U.S. global leadership around the free and open Internet, including promoting cross-border data flows. Digital trade has become an engine of economic growth for large and small businesses around the world, and the flow of data now contributes more to GDP growth than the flow of goods.

Some countries have taken steps to limit cross-border data flows through forced data localization requirements. Such requirements fail to recognize the way that modern distributed networks function and could have the unintended consequence of weakening privacy and security protections (*https://www.blog.google/products/google-cloud/freedom-data-movement-cloud-era/*). A comprehensive Federal data protection law that eschews data localization would serve as a bulwark against data localization requirements and lend credence to the idea that countries can protect privacy on a cross-border basis without compromising key digital trade principles. A Federal law could also build on recent steps taken by the US, Mexico, and Canada in the USMCA to require protection of the personal information of users of digital trade and to promote compatibility between different privacy frameworks. As NTIA recognized in its request for comments, it is important to promote a regulatory landscape that is consistent with international frameworks for protecting privacy, including the APEC Cross-Border Privacy Rules System.

Question 5. Also included in NTIA's request for comments, how should the U.S. Government encourage more research and development of products and services that improve privacy protection?

Answer. We believe the Federal Government has an important role to play in enabling the development of privacy and security enhancing technologies.

We encourage the Federal Government to continue providing funding for the research and development of products, services, and techniques that improve privacy and security protection. Basic research remains cost intensive and educational institutions and research organizations need sustained funding to make the critical long-term investments that lead to new and improved ways to protect privacy and security. However, in its support, the government should not only focus only on the products and services that consumers see as an end-result, but also on expanding the types of tools and training available to practitioners. For example, techniques for internal data management and expanded availability of ethics training in schools can promote better outcomes for consumers.

The government should also consider establishing local centers of excellence for privacy and security research and applications, perform privacy and security research at government labs and agencies, create frameworks and mechanisms to facilitate public-private sector collaboration, and explore incentives for researchers who receive public funding to explore priority areas of research. Google has long

supported open-source research, and we encourage open access to publicly funded research.

In addition the U.S. Government should leverage its convening power to disseminate best practices to ensure that every organization that processes personal data, including the government itself, can keep abreast of and implement the state of the art. Publications, public events, technical workshops, digital literacy programs, and advisory committees, are potential ways the government could achieve this goal.

Lastly, the U.S. Government should leverage its convening power to disseminate best practices to ensure that every organization that processes personal data, including the government itself, can keep abreast of and implement the state of the art. Publications, public events, technical workshops, digital literacy programs, and advisory committees, are potential ways the government could achieve this goal.

Question 6. 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. The GDPR requirements of 'right to portability' and 'right to be forgotten' are separate concepts and we would encourage policy makers to consider them apart from each other.

With regard to user control, we believe that individuals should retain control over personal information, including when used as an input into proprietary machine learning or other algorithms.

However, we take into account privacy design principles in our development and deployment of machine learning or other algorithms, including to first see if the algorithms can be effective using anonymous data rather than personal information. For example, Google can input an aggregate of users' search queries into algorithms to learn about which search results are most relevant to which queries, without the need to include specific user information or store outputs in a way connectable to a specific user.

If the function of the algorithm does require the use of personal data, we aim to provide the user with transparency and control. So, for example, Google's algorithms use a specific user's search history (if their settings permit it) to predict the best search results for that user. Such uses can be managed, in Google's case, through easy-to-use tools for individuals to delete data stored in their account. This will cause future predictions to exclude the deleted data.

Methods like these can enable systems to continue to work and innovate while still keeping individuals in control.

Question 7. 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. At Google, we view all information tied to an identified individual as "personal information", whether it is information they provided to us, information our systems associated with them, or outputs of our algorithms. For example, our advertising systems sometimes attempt to determine topics of interest for a signed-in user based on his or her activity. These results are available to see, change, and delete in Ad Settings, and we consider them personal information.

Question 8. Since companies often use aggregated data outputs to study and improve their existing algorithms, services, and products, what impacts do you expect these vague GDPR requirements to have on companies' abilities to innovate?

Answer. The GDPR helpfully excludes data that is no longer capable of being associated with an individual. It also creates specific exemptions for "pseudonymized" data for research purposes. While we will learn more about how these provisions will be interpreted, we generally think this principle is the right one: the law should encourage organizations to store and use data in the least identifiable manner that is compatible with the purposes for which it collected it.

Question 9. In July 2018, I joined my colleagues Senators Thune and Wicker in a letter to Google requesting more information on the data privacy practices of their Gmail service, and more specifically, third party app developers' access to e-mail contents. In response to questions posed in our letter, Ms. Susan Molinari, Vice President of Public Policy and Government Affairs of Americas Google Inc., indicated that the verification process of third-party web apps that request access to sensitive data, such as the contents of Gmail message, undergo manual reviews of the app's privacy policy and the "suitability of the permissions the app is requesting." Will you please further explain the specific considerations of the manual re-

view process as it determines the "suitability of the permission the app if requesting?"

Answer. As we describe in our previous response, developers that request access to sensitive data, like Gmail data, must complete a verification process, described at *https://developers.google.com/apps-script/guides/client-verification.* This process is designed to prevent apps from misrepresenting themselves to users or accessing data that they do not need in order to perform their function. That process involves a manual review of the app's privacy policy to ensure that it adequately describes the types of data it wants to access and a manual review of the suitability of permissions the app is requesting compared to its functionality.

Google's proactive review also includes the use of machine learning tools to detect metadata signals that could indicate an app is malicious. Depending on the results and a developer's history and user feedback, we identify apps that need additional manual review for verification. This review can include testing their app directly, reviewing their website materials, among other investigative steps.

In addition, we are launching stricter limits through our appropriate access policy. Starting in January 2019, we will only allow specific types of applications—such as e-mail clients and productivity tools (the new policy is available at *https://developers.google.com/terms/api-services-user-data-policy#additional-requirements-for-specific-api-scopes*)—to access certain Gmail APIs. In addition, when users grant Gmail access to applications that do not require regular direct user interaction (for example, services that provide background reporting or monitoring to users) users will be provided with additional warnings, and we will require them to re-grant access at regular intervals.

We are also continuing work to ensure compliance with our policy that developers should only request access to information they need. During application review, we will be tightening our review for compliance with this existing policy. For example, if an app does not need full or read access and only requires send capability, we require the developer to request narrower permission scopes so the app can only access data needed for its features.

Finally, our new policies add strict limitations on how data may be used. Apps accessing these APIs can only use Gmail data to provide prominent, user-facing features and may not transfer or sell the data for other purposes such as targeting ads, market research, e-mail campaign tracking, and other unrelated purposes. (And Gmail users' e-mail content is not used by Google for ads personalization.) As an example, with a user's permission, consolidating data from a user's e-mail for their direct benefit, such as expense tracking, is a permitted use case. However, consolidating the expense data for market research that benefits a third party is not permitted. We have also clarified that human review of e-mail data must be strictly limited.

Question 10. Ms. Molinari's response also indicated that Google's Security Checkup Tool described in the letter would flag unverified apps for users. From the descriptions and graphics provided in the response, it remains unclear exactly the granularity of information that is relayed to the consumer in checking on the status of a third-party app and its access to their data. For instance, does third-party access to sensitive information to Gmail, Google Calendar, Google Contacts, and Google Hangout allow the third-party to retain the data for a certain period of time? If the consumer opts-out of sharing sensitive information with the third-party shown on the Security Checkup Tool, is that information deleted immediately, and if not, how long is it retained before deletion?

Answer. As described in our previous responses and in our Help Center (available at *https://support.google.com/accounts/answer/3466521?hl=en*), to help users safely share their data, Google lets them give third-party sites and apps access to different parts of their account. By visiting their account permissions page (available at *https://myaccount.google.com/permissions*) or using Security Checkup, users can review and control all apps that have access to their account, including viewing exactly which permissions each app currently has. If a user gives account access to a site or app they no longer trust or otherwise want to remove, they can remove its access to their Google Account at any time. That site or app won't be able to access any more information from the user's Google Account, but the user may need to request that the third party delete the data they already have.

Question 11. In the response, Ms. Molinari explained the most common reasons for Google suspending or removing third-party apps' access to Google customers' sensitive information should they fall out of compliance with Google's policies. Our original inquiry in July requested a list of all instances in which Google has suspended an app in this way, with an explanation of the circumstances for each. Will you please provide this list in your written response for the committee record?

Answer. We support our policies on third party access to Gmail user data with verification, monitoring, and enforcement. In addition to the measures described in our previous response, Google's proactive review of apps seeking access to user data also include the use of machine learning tools to detect signals indicative of malicious apps. Depending on the results, a developer's history, and user feedback, we identify apps that need additional manual review. This review can include testing their app directly and reviewing their website materials, among other investigative steps.

In addition, we recently announced even stronger privacy controls. These controls include an improved user permission flow that provides a finer-grained ability to choose what data they share, limiting the types of apps that can request access from Gmail users, and imposing new requirements on how developers must treat Gmail data. These policy changes are going into effect on January 9, 2019.

More specifically, beginning in January 2019, we will only allow specific types of applications—such as e-mail clients and productivity tools (the new policy is available at *https://developers.google.com/terms/api-services-user-data-policy#additional-requirements-for-specific-api-scopes*)—to access certain Gmail APIs. When users grant Gmail access to applications that do not require regular direct user interaction (for example, services that provide background reporting or monitoring to users) users will be provided with additional warnings and be required to re-grant access at regular intervals.

We are also continuing work to ensure compliance with our policy that developers should only request access to information they need. During application review, we will be tightening our review for compliance with this existing policy. For example, if an app does not need full or read access and only requires send capability, we require the developer to request narrower permission scopes so the app can only access data needed for its features.

Finally, our new policies include additional, strict limitations on how data may be used. Apps accessing these APIs can only use Gmail data to provide prominent, user-facing features and may not transfer or sell the data for other purposes, such as targeting ads, market research, e-mail campaign tracking, and other purposes unrelated to these features. As an example, with a user's permission, consolidating data from a user's e-mail for their direct benefit, such as expense tracking, is a permitted use case. However, consolidating the expense data for market research that benefits a third party is not permitted. We have also clarified that human review of e-mail data must be strictly limited.

As one example of how Google enforces its policies, in June 2018, we identified an app in our verification and review process that appeared to imitate another legitimate company. The deceptive app claimed to make sending and receiving e-mails easier. Our review identified that the app had no apparent functionality. In addition, the app exhibited numerous suspicious signals. For example, the app's login page simply redirected users to their Gmail page and was otherwise nonfunctional. The app also claimed to have a demonstration page for users that did not actually exist. The app's request for verification was rejected and the app was suspended from requesting user data.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELLEY MOORE CAPITO TO KEITH ENRIGHT

Question 1. According to a study by Pew Research, only 38 percent of consumers know how to limit what information they give online. Consider me among those consumers who do not know what is being collected and how to keep my information to myself. Even with privacy settings and assurances that my data is not being collected and used without my consent, I still have concerns.

I believe the root of this issue is transparency and consumer confidence. What are your companies doing to increase the transparency when it comes to the type of data you collect?

Answer. Transparency is a core principle, and we provide users with clear, simple explanations of what we collect and our use of it. We realize privacy policies aren't user's first choice of reading material, but we worked to make ours best-in-class, with illustrations, videos and other interactive content designed to convey key concepts and choices.

But we go beyond transparency to try to really help users understand, in real time and in context as they use our services. We gave some examples in my testimony, and just last week added new transparency in our flagship product, Search, that shows users exactly how their data is being used to improve their search re-

sults, along with direct access to controls. (*https://www.blog.google/technology/safety-security/making-it-easier-control-your-data-directly-google-products/*)

Question 2. What difficulties have your companies faced when developing more transparent privacy policies?

Answer. We value being transparent with our users about how and why we use data to operate our business. Making this information available is critical to building and maintaining user trust, and specifically helps our users make important decisions about their privacy. One challenge we have encountered is how to ensure users have the information they need, without overwhelming them with extraneous details. We are constantly refining this balance based on feedback from our users.

We recently updated our privacy policy to incorporate some of the insights we have gained.

While we don't solely rely on the privacy policy for that purpose, we still want to make our policies understandable and accessible to users who spend the time to review them as well as being full and complete statements of our data practices for experts and regulators to hold us accountable. We try to meet both needs, via clear headings, easy navigation, overlays and examples, and explanatory videos.

We regularly conduct surveys and interviews with users to inform our approach and ensure we strike this balance effectively.

Question 3. West Virginia has a high elderly population that is rapidly increasing as baby boomers retire. I am positive that a lot of my elderly constituents are among those individuals who do not know how to limit their online information.

What are some of the measures your companies are doing to teach consumers—and specifically older consumers—about what data they share on your platforms?

Answer. Google invests directly and through partnerships with expert organizations to inform individuals about the data they share on our platforms, and ways to protect their privacy and security. In addition to our efforts on transparency mentioned above, we offer Privacy Checkup (*https://myaccount.google.com/privacycheckup*) and Security Checkup (*https://myaccount.google.com/intro/security-checkup*). These tools are helpful for all our users, but we believe seniors who feel less comfortable with online services could particularly benefit from the guided review of their privacy and security settings.

In terms of partnerships, we support organizations that provide general audience and senior-specific digital literacy information, through financial assistance, take-home kits that include security keys for two-factor authentication, and general privacy and security advice. For example, we helped support ConnectSafely's development of the Senior's Guide to Online Safety (*https://www.connectsafely.org/seniors/*).

Project GOAL (Getting Older Adults Online) is an organization dedicated to helping older adults access broadband and address barriers like digital literacy to making that possible, safely. We have provided financial support to Project GOAL to support their work to educate older consumers and to generally raise the profile of this important work.

Question 4. I know advertising through data collection has a monetary value, and appreciate the business model, however, I find it hard to know what is being collected and how I can keep my information to myself. Even with privacy settings and assurances my data is not being used without my consent, I still have concerns.

Please explain how your business model allows both data to be used to make suggested recommended purchases on your site? As well as how you use that data to target ads to consumers? And how do you do that while protecting personal data?

Answer. The online advertising model enables advertisers to reach audiences who are more likely to be interested in purchasing their products or services, and therefore to waste less of their marketing budgets on audiences who are not. This model has lowered barriers to entry for scores of small businesses, enabling them to compete for access to global markets.

At Google, supporting this economy while promoting the privacy and security of user data is essential. Crucially, users' personal information stays within Google and is not shared with or sold to advertisers. Advertisers instead have access to our services through dashboards and other interfaces that enable them to decide how to show ads to aggregated audiences with certain characteristics.

While providing free, ad-supported services, we remain committed to putting users in control of their privacy, so we are constantly improving our privacy disclosures, settings and controls. Users can opt out of personalized ads via Ad Settings and the AdChoices industry program, via a notice served in every ad Google shows.

Our Ad Settings page not only allows you to turn off targeted ads; it also shows you what data we use to personalize ads, as well as the topics and advertisers we think you are interested in (and why we think you are interested).

Our industry-leading policies prohibit the use of sensitive categories for ad targeting. As we explain to users in our privacy policy, we do not show personalized ads to people based on sensitive categories, such as race, religion, sexual orientation, or health conditions. And we don't allow advertisers to use these sensitive interest categories to select audiences for their ads.

Building systems that users trust is essential to the continued success of Google and the Internet at large. So, we keep the information we collect confidential and under users' control, and work every day to maintain that trust.

Question 5. How can Congress ensure that data collected is used responsibly without shutting down the collection of data completely?

Answer. While companies and regulators like the FTC are doing a lot today to protect privacy and security, we think it is has long been appropriate to adopt a comprehensive data protection law in the United States. Our model framework includes a set of principles, based on established regimes like the Fair Information Practices Principles (FIPPs), OECD Privacy Principles, Asia-Pacific Economic Cooperation (APEC) Privacy Framework, and aspects of the European General Data Protection Regulation (GDPR). We also bring our 20 years of experience offering services that depend on information, privacy protections, and user trust.

We specifically urge a law that requires organizations to be responsible to individuals whose data they collect:

Organizations must operate with respect for individuals' interests when they process personal information. They must also take responsibility for using data in a way that provides value to individuals and society and minimizes the risk of harm based on the use of personal information.

We think an approach like this can bolster trust and use of online services in a way that still encourages new and innovative uses of data.

Question 6. In April, the European Union (EU) passed the General Data Protection Regulation (GDPR) in order to protect personal data and uphold individual privacy rights. These new regulations have created uncertainty for U.S. firms, despite several already coming into compliance.

Innovation is important to small businesses, especially in rural America. The new European standards have created massive hurdles for these businesses to be in compliance. Many small companies in Europe are already expressing an inability to afford the legal consequences. For example, if a rural grocery store advertises online and provides a link to coupons. Under the GDPR compliance rules, this simple practice can result in expensive legal consequences.

For those who do business in Europe, do you think GDPR has the potential to have negative impacts on rural small businesses in Europe?

Answer. We do worry about the impact of data protection regulation on small businesses and new entrants, who lack the resources to build complex compliance programs like Google has built. This would be a bad outcome for everyone.

This difficulty can be managed, in our view, with flexible regulation that focuses on the principles of accountability and protecting users from harm. There should be many ways to demonstrate accountability, which scale with the size and scope of the organization. For example, small businesses should have access to industry best practices, or open-source projects for obligations like data portability, that can allow them to meet the requirements of the law without significant cost or expertise.

Question 8. California has already passed a sweeping consumer protection law that threatens established business models throughout the digital sector. I appreciate the industry taking the initiative in creating a framework, in addition to the privacy principles released by the U.S. Chamber of Commerce.

As we begin discussing the appropriate position of the Federal Government, can you describe what actions we should investigate more closely for any potential national framework?

Answer. As you consider creating a Federal framework, we hope you will also take into account our model framework, as we referenced above, which sets out substantive requirements and enforcement and scoping principles. An important component of our framework is the principle that new privacy regulations should apply across the board, to all sectors of the economy.

Question 9. Who, in your opinion, is the appropriate regulator to oversee any framework and why?

Answer. Many different regulators have been involved with data protection in recent years, and they all have an important role to play in the future. In particular, the Federal Trade Commission has been the primary Federal privacy regulator, and have built a track record of strong enforcement and deep expertise on this issue.

Question 10. According to recent research by Magid, a media research firm, 35 percent of millennials share their password to access streaming services. I certainly

understand that the terms and conditions of these services already note that access is for personal use and not to be shared with others. And that the account holder remains responsible for the actions of that third party. However, as the number younger generations sharing their password grows so has the potential for abuse. This "overly sharing of passwords" and the younger generation operate differently than many my age.

Are your policies flexible to cover a third party that may use a friend's or spouse's password? Is this something we should consider as we create Federal guidelines?

Answer. We strongly discourage password sharing which can create serious security and other problems for those involved. We have mechanisms for families to share content via their Google Family Group, which allows users to share apps, movies and books through the Play Family Library or subscriptions like YouTube Premium and Google Play Music.

For shared devices like Google Home, others in your home can request music from the device if you have logged into the device with your personal music account. We ask users for additional permissions before surfacing sensitive information like calendar entries (*https://support.google.com/googlehome/answer/7684543?hl=en&ref_topic=7549809&visit_id=636764503506028117-3686497603&rd=1*) or payments (*https://support.google.com/googlehome/answer/7276665*).

We created Be Internet Awesome (*https://beinternetawesome.withgoogle.com/en*), our flagship digital literacy program, to give younger users the knowledge and tools to navigate the Internet safely. One of the five lessons, Be Internet Strong, specifically teaches kids to not share passwords with anyone other than parents or guardians. We worked with the Family Online Safety Institute and ConnectSafely as well to build a program that aims to encourage parents, educators and kids alike to exhibit all the traits that comprise "Awesome" online: to be Smart, Alert, Strong, Kind and Brave.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO KEITH ENRIGHT

Question 1. GDPR establishes a right of data portability, which some believe is key to driving new innovation and competition within the emerging data ecosystem. Others are concerned that data portability rights, depending on how crafted, could further entrench incumbent companies.

What questions should policymakers be asking in developing data portability rights?

Answer. Google strongly supports the notion that users should be able to export the personal information they have provided to an organization, in a format that allows them to understand the information, store a local copy, and/or to import it into another provider's systems. This has two important consumer benefits. First, it empowers individuals to understand and control their personal information. It also keeps the market innovative, competitive, and open to new entrants by allowing users to easily move to new services without losing the benefit of their accumulated data.

More generally, we have worked on portability for over a decade and were the first to offer a portability tool in 2011. We updated and broadened this tool, Download Your Data, last spring so that it now covers more products and data types. The tool allows users to take personal information about them stored in more than 50 Google products, including search queries, Gmail messages and contacts, YouTube videos, and many others. The output is provided in formats designed to be importable into software on the user's own devices or other services.

The ability for users to transfer data directly from one provider to another, without downloading and re-uploading it, is a significant advancement in making portability practical for users all over the world. We are working with partner companies on the Data Transfer Project (*https://datatransferproject.dev/*), an open-source initiative to expand this capability and make it even easier for users to try a new service or otherwise control their data. The current partners (Google, Microsoft, Twitter, and Facebook) are working on building a user interface as well as bringing new and more diverse partners into the project.

Question 2. What improvements would you make, if any, to Art. 20 of GDPR, which addresses the right to data portability?

Answer. This is the very early stages of GDPR enforcement, and so we cannot tell precisely how this provision will be interpreted and enforced. We agree it will be important to continue to observe the experience of data portability under the GDPR to best learn what is working well and what can be improved.

The GDPR's portability provision applies to personal data "provided to a controller", avoiding data types like inferred data or observed data that often cannot be practically made available for download. While some observed or inferred data can be made available (and we do so in Download Your Data), it may not be appropriate to mandate such a requirement. Our model principles follow a similar line.

Question 3. How best can data portability rights be crafted to create new competition, but not further entrench incumbent companies?

Answer. Our proposed privacy framework suggests applying general principles in ways that reflect the different resources of different organizations. The overall touchpoints should be accountability and preventing harm, rather than inflexible one-size-fits all rules. Accordingly, we urge the Committee to explore ways to develop the data portability principle to work for businesses of all types and sizes.

One way to further this goal is for industry organizations and government entities like the Federal Trade Commission to explore best practices and methodologies that can be adopted by smaller players—perhaps via open-source projects or other low-cost options.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO KEITH ENRIGHT

Question 1. Does the Google "my activity" page make all data collected available to each user? Does Google collect information that is not reflected in "my activity?"

Answer. Our goal with My Activity is to allow users access to all the personal information we collect about the user across our services. We are adding more sources over time, but we are not able to provide every piece of data, for a few reasons:

- The Google Account is only available to users who sign in to an account, and not to users who we recognize only via a pseudonymous cookie or device ID. We do not have a secure way to provide such access to unauthenticated users. Users who are not signed-in have other ways to control their data we collect about their use of our services and devices.
- We don't want to overwhelm users with detail, so might show a single event (*e.g.,* a search query), when we log several interactions (*e.g.,* the initial page load, the query, each page of results).
- Some data is stored only on a temporary basis—hours or days—before being deleted.
- Some activity is not yet technically possible to share, because of changes to infrastructure, new products that have been released, or other technical limitations. We aim to reduce this category of information over time.

Question 2. Does Google Home collect and use sensor data to infer consumer activities or interests? Is this information used for advertising or marketing purposes? If so, how is this information processed and stored? Can consumers view this data and/or opt-out of this data collection?

Answer. We realize our users want to keep their private spaces private, and our Google Home devices are designed with that in mind. We do not send voice data to Google unless the user activates the device.

When Google Home's microphone detects that a user has said the hotwords "OK Google," or "Hey Google", the LEDs on the device light up (or on Google Home Hub the Google Assistant visually transcribes your request on screen) to tell you that recording is happening. Google Home records what you say, and sends that recording (including the few-second hotword recording) to Google in order to fulfill your request.

Google uses the data it collects to make our services faster, smarter, and more useful to users, such as by providing better search results and timely traffic updates. Data also helps protect users from malware, phishing, and other suspicious activity. For example, we warn users when they try to visit dangerous websites.

Note that search queries made via Google Home, just like those entered via Google.com, can be used to select ads as well as search results. To do this, we use the text of the query, not the voice recording of our user. In general, we use data to show ads that are relevant and useful to the user, and to keep our services free for everyone.

Google stores data about users' interactions with Google Home on its servers, which reside in its data centers. Users can view and delete interactions (or all conversation history) with the Google Assistant in My Activity. Users can also edit the information they allow Google Home to access in their Settings.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO KEITH ENRIGHT

Question 1. When devices get old they get to a point where they cannot support updates for the device the operating system or the many applications run on the device. What is the obligation of the device manufacturer's, operating system programmers, and app developers and programmers regarding to older devices?

Answer. Pixel and Nexus phones—devices where Google is the OS provider—receive security updates for at least 3 years from when the device first became available on the Google Store, or at least 18 months from when the Google Store last sold the device, whichever is longer. Android version updates for the Google Pixel 2 and 3 are guaranteed for at least 3 years from when the device first became available on the Google Store, and for 2 years for older Nexus and Pixel devices.

We publicly announced this policy in 2015 (see *https://android.googleblog.com/2015/08/an-update-to-nexus-devices.html*) and provide detailed information about update periods in our help center at *https://support.google.com/nexus/answer/4457705?hl=en.*

We are limited in our ability to push out updates to Android devices offered by other providers. We have worked with carriers and OEMs to help reduce friction for updates, although ultimately work must be done by the provider to make an update available to end users.

Question 2. What guidelines do your companies follow when it comes to communicating with consumers when either the hardware or software they are using can no longer support updates—especially when these updates relate to security? Is there an industry wide practice that applies here?

Answer. We provide detailed information about update periods in our help center at *https://support.google.com/nexus/answer/4457705?hl=en.* We aren't aware of standard industry practice in this regard, but at Google we continue to review and update our practices with respect to communicating updates notifications to users.

Question 3. What is a reasonable consumer expectation with regard to how long the device will be viable?

Answer. For devices like smartphones, we lay out to customers what they can expect in terms of support. See our help center at *https://support.google.com/nexus/answer/4457705?hl=en*

Question 4. The EU has considered promoting a voluntary labeling system informing consumers about a product's durability, upgradeability and reparability. What do you think of this idea?

Answer. We are strong supporters of making information available to users that will help them to better understand and secure the technology they use. For example, we recently refreshed our Safety Center, adding new guidance on security, privacy, and safety. (You can access it at https://safety.google/) We have been in discussions with a number of stakeholders regarding various "labeling" efforts. There are challenges in providing a useful set of standardized information, however, we continue to look for ways to provide this type of useful information.

Question 5. Should devices come with an expiration date in order to manage consumer expectations and more importantly their awareness of their online safety?

Answer. As noted above, we believe in providing consumers with the information they need to help make important decisions about their Google smartphones. For instance, we tell users how long their Google devices will be supported with guaranteed security updates. (See *https://support.google.com/nexus/answer/4457705?hl=en*)

Users of Android devices can always check the device's Android version number and security update level in the Settings app, which can help them to verify that it is operating the latest software.

Question 6. I'm very concerned about the use of consumer data for uses that we did not sign up for. Google recently released general basic principles for privacy—What part of the privacy principles Google has developed, is focused on the aspect of data security that I mentioned?

Answer. Security is a primary requirement for any data protection regime. Our data protection framework (*https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf*) notes that all organizations must implement reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, modification, and destruction, and should expeditiously notify individuals of security breaches that create significant risk of harm. Baseline precautions should apply to any collection of personal information, and additional measures should account for and be proportionate to the risk of harm.

Question 7. Do you think separate privacy principles are needed to address the parts of data security that are invisible to consumers like research?

Answer. Security should apply to all processing of personal information, whether visible to consumers, for research, or in any other manner. Our expectation is this can be accomplished with a general principle as above.

Question 8. In general we have been exploring the idea of opt in frameworks to keep consumers informed about what their data is being used for. However, we know from recent history that there are some uses of data that should never be permitted—like the leveraging personal data to interfere with election processes. How could we design an opt in framework that is meaningful to consumers, doesn't desensitize them to important decisions about privacy and makes sure they consent only to lawful uses of their data?

Answer. Google believes in ensuring our users understand how their data is used, and are in control. Consent is particularly important for data uses that involve a high risk to users and might not be well understood based on context. While controls are vital, there is a growing consensus amongst regulators, researchers, and companies that asking users to opt-in for all uses of information is impractical and leads to fatigue that diverts attention from the most important choices.

For example, some data processing is necessary to make products work, and to ensure they're secure and reliable. Users expect these uses as a result of using a service, and asking them to consent in addition presents the odd decision of "agree" or "don't use the service." This could have the perverse effect of teaching users to simply click "agree" to everything without paying attention.

Other data uses are not necessary for a service, but support the service provider's interests without posing significant risks to users. In the parlance of the GDPR, these "legitimate interests" appropriately balance the rights and interests of individuals without requiring specific consent.

We urge your office and Congress more generally to consider different levels of control, rather than an one-size-fits-all approach. The GDPR's approach, with multiple valid bases for processing personal data, is a useful starting point.

Question 9. Short of regulation, what more can you and your colleagues and competitors do to restore and maintain our and our constituents' trust that you won't continue to collect more data than consumer understand, use it in ways they never imagined, and then fail to protect the data from unauthorized use and access?

Answer. We share your concern that recent incidents and news reports have damaged user trust, and we are working hard to restore it, at least where Google is concerned. A comprehensive Federal data protection framework will help in this regard, but in the interim we continue to build out transparency and user controls, and our internal privacy program.

For example, last week we added new transparency in Google Search that shows users exactly how their data is being used to improve their search results, along with direct access to controls. (*https://www.blog.google/technology/safety-security/making-it-easier-control-your-data-directly-google-products/*)

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO KEITH ENRIGHT

Question 1. State Preemption: Several public interest organizations have written the Committee in advance of the hearing expressing their deep concerns about state preemption. As the ACLU noted, it has often been the states—not the Federal Government—that have acted in a timely and important way to protect consumer interests.

Please provide to me a set of recommendations for how to improve the California Consumer Privacy Act and the GDPR.

Answer. We support thoughtful privacy legislation that both protects consumers and encourages businesses to continue innovating.

With regard to the recently enacted California Consumer Privacy Act (CCPA), we support the goals of the law, including increased transparency and user control, but share the concerns that many have expressed about how the law is drafted and its impacts on businesses and consumers. In particular, we hope that the law can be clarified to make it easier for consumers to understand and exercise their rights, and ensure that companies of all sizes and sectors can comply and continue to offer innovative products and services consumers rely on.

At the same time, we believe the CCPA does not go far enough in codifying the rights and obligations included in consensus frameworks such as the Fair Information Practices Principles (FIPPs), OECD Privacy Principles, APEC Privacy Framework, and even Europe's General Data Protection Regulation (GDPR). We recently

put forward principles for a responsible data framework (*https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf*), based on the aforementioned frameworks, and our 20 years of experience offering services that depend on information, privacy protections, and user trust.

While we don't agree with everything in the GDPR, and indeed there are aspects of it that reflect specific European standards that aren't globally applicable, the Regulation does rest on global fair information practice principles that also inform our model framework. For example, the GDPR includes requirements of transparency, user control, data quality, and security, to name a few.

In particular, we would point to the GDPR's concept of a "data processor" versus "data controller" as a useful way to distinguish providers of general consumer services from enterprise services that act as "vendors" for others, without independent rights to process data on their own behalf. This concept is a helpful way to allow for the efficient use of vetted, qualified vendors with minimal additional compliance costs, which is particularly important for smaller entities. Processors can look to the controller to meet certain obligations under the law, including transparency, control, and access, but processors must still meet basic programmatic and security responsibilities.

We also support the GDPR's notion of "legitimate interests" as a positive way to permit standard or typical data uses that are consistent with individuals' interests while reserving express consent to those situations where users really need to pause and consider their choice.

Question 2. Privacy by Design: Between the six of your companies, you have access to an overwhelming amount private information about nearly everyone in the United States. AT&T and Charter have access to the browsing history of your customers. A Princeton study found that Google collects visitor data from 70 percent of websites—including from Twitter, a competitor. It's hard to imagine what your companies don't know.

Would you commit to privacy-by-design—limiting collection of data and deleting data when it is no longer useful to your customers?

Answer. Integrating privacy into product design and abiding by reasonable limitations on data collection, use, and disclosure are key principles of a data protection regime. As we noted in our responsible data protection framework, we believe that any law should:

Place reasonable limitations on the manner and means of collecting, using, and disclosing personal information. Collection and use of personal information can create beneficial and innovative services, within a framework of appropriate limits to the collection, use, and disclosure of personal information to ensure processing occurs in a manner compatible with individuals' interests and social benefits.

Question 3. What specific steps do you plan to take to limit your own use of customer data? Can you provide examples where you deleted or stopped collecting data to protect privacy?

Answer. At Google, we design our products to ensure that data collection and use happen only as necessary for the purposes of the products and stored no longer than necessary for those purposes. This principle can be seen in virtually every product we make, but for example:

- Our logs, which record interactions with our services, store personal information only as long as necessary. Some logs are kept for days or weeks only. Logs for our advertising services are anonymized by removing part of the IP address (after 9 months) and cookie information (after 18 months).
- Recently, we determined that we no longer needed to process Gmail information for the purpose of selecting ads, and changed our product behavior accordingly.
- We run many models on device, including translation in Google Translate, optical character recognition in Android Pay, face detection in StreetView to blur faces, and offline speech recognition. On-device processing makes features available to offline or low-bandwidth users, reduces latency, and maintains all data on-device—it is not collected by Google.
- All development of AI technology at Google—e.g. computer vision and speech recognition—and use in our products and platforms to make the technology available externally, including through the Google Cloud suite of APIs, must meet our standards for privacy and general responsible technology development as laid out in our AI Principles (*https://www.blog.google/technology/ai/ai-principles/*).

Question 4. Privacy by design is fundamental to the GDPR. What specific changes have you made to your products to come into compliance to the GDPR's privacy-by-design requirements?

Answer. Our services are built from the ground up with privacy in mind. This has been part of our internal privacy program for years, and was the basis for our GDPR compliance effort. As we described above, we have introduced many privacy enhancements to our products.

Question 5. FTC Rulemaking: In most of your remarks, you discuss the challenges of regulating evolving technologies and economies. It would seem to me that this requires a Federal agency that is responsive to technology changes.

Would you support the FTC having rulemaking authority to provide clarity, to address potential harms, and to ensure rules match technology changes? What sorts of areas should this cover?

Answer. This question is an important aspect of the process to develop comprehensive baseline privacy legislation and we would welcome the opportunity to work with you as that process develops. In particular, the FTC should continue to investigate and help organizations understand the types of harms that can occur from the misuse of data, including ones that are not specifically monetary.

Question 6. Advertising and Tracking: With ad blocking penetration approaching 20–30 percent, consumers are clearly concerned with how their data is used for advertising and tracking.

Approximately how many websites or what percent of major websites does Google have any sort of tag capable of tracking a user?

Answer. Google has millions of customers who use our advertising services to generate revenue to support their websites and apps. These services generally involve Google recognizing the user or user's device using a cookie or similar technology. We unfortunately do not have data on the percentage of sites or apps using our advertising services.

An even larger number of websites and apps use Google Analytics to learn about visitors to their sites and apps. Note that our standard analytics products are not used to identify a user *across* websites or apps, but merely to provide analytics services to a specific publisher or developer.

With regard to ad blocking, Google is a member of the Coalition for Better Ads (CBA), an industry organization which focuses on improving users' experience with advertising. Through research, the CBA has identified poor user experience and annoying ad formats as the top driver of ad blocking and developed standards to address these issues. Google supports these efforts by using Chrome to implement the CBA standard and filter offending formats.

Question 7. Considering web browsers do not need to allow for tracking, has Chrome considered rolling out Intelligent Tracking Protection (ITP) like functionality? If not, why doesn't Chrome introduce it?

Answer. Google is deeply committed to user privacy and keeping our users' trust is core to everything we do. Google Chrome already offers our users the ability to control cookies and their online browsing experience. You can delete existing cookies, allow or block all cookies, and set preferences for certain websites. Users can also opt out of personalized ads via Ad Settings and the AdChoices industry program, via notice served in every ad Google shows.

We will continue to respect users' preferences, including cookie controls, and work with browser vendors and those that depend on online advertising—like news publishers—to find solutions that work for everyone.

Question 8. Much of Google's advertisements on its own properties are whitelisted as part of the so-called "Acceptable Ads" program. Please describe this program: what specific partners participate and what incentives are provided to participants?

Answer. We are one of a number of digital ads providers who are a part of Eyeo GmbH's (also known as "AdBlock Plus") Acceptable Ads program (*https://adblockplus.org/en/acceptable-ads#criteria*). Under the program, AdBlock Plus decides whether a company meets its acceptable ads criteria.

AdBlock Plus has found that Google Search ads meet these guidelines, so it whitelists Search ads. However, the Acceptable Ads program does not cover Google's display ads, or the display ads we select for placement on third-party websites. Those may be still blocked by AdBlock Plus.

Even though the Acceptable Ads program covers only a portion of Google Ads, we pay AdBlock Plus, which requires such payment from large companies.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO KEITH ENRIGHT

Question 1. Unsurprisingly, none of your testimony speaks about potential increased penalties for a new privacy framework. The current penalty regime seems not to change corporate behavior—as we repeatedly have seen. In your opinion, are civil penalties an effective mechanism to push companies to follow the law? If not, what mechanisms would be effective?

Answer. This question is an important aspect of the process to develop comprehensive baseline privacy legislation and we would welcome the opportunity to work with you as that process develops.

Our privacy framework (*https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf*) suggests tying enforcement to risk of harm to users, such that penalties, including civil fines, should be proportionate to the risks to users posed by the behavior or failure in question. This creates the right incentives for businesses without over-penalizing technical violations of the law that pose little or no risk to users.

Question 2. Does Google track browsing and location history for Google for Education users or for children's accounts governed by FamilyLink?

Answer. Our K–12 G Suite for Education users are treated with particular care, and while we collect information in order to operate these services, our policy prohibits the use of any personal information from such users to target ads, whether in the core G Suite services or even when using our additional consumer services, like YouTube. These accounts also do not have an option to enable the Location History product, unless specifically enabled by an administrator. You can read more about our privacy practices for these accounts at *https://gsuite.google.com/terms/education_privacy.html*.

Parents have the ability to manage their children's use of Google services via Family Link, including setting website restrictions, activity controls (like Web and App Activity that covers collection of browsing history) and location settings. As with G Suite accounts for Education, we block personalized advertising for users under the age of 13. Device location information may be collected depending on the device and account settings set by their parent. In Family Link, parents may choose to enable device location in order to be able to see the most recent location of their child's device. We collect this information to provide this service, and do not store this location information long term. However, the location of a child's device may be stored with their search activity if Web & App Activity is enabled for their account. This data is used to do things like provide more relevant search results. Parents are able to review and delete their child's activity. You can read more about these accounts at *https://families.google.com/familylink/privacy/notice/*.

Question 3. How does Google process and store this data? Does Google make interest profiles visible to the users of their parents? Does Google provide users or their parents with a way to opt-out of this data collection?

Answer. As we described above, Google does not develop ad profiles or use personal information to target ads to children using these accounts. Information of G Suite for Education users is accessible by the school administrators, and for accounts for users under 13, by parents. With Family Link, parents have the ability to modify their child's data collection settings and/or review their child's data by signing in to their account.

Question 4. If a Google for Education User or a child FamilyLink account holder converts their account into a regular personal Google account, does Google use browsing and location data from the Education/FamilyLink account to serve ads to the personal account?

Answer. There is no mechanism at this time to convert a G Suite for Education account to a regular consumer account. G Suite for Education does enable students to copy their content from their school account to a regular account so they do not lose their school work when they graduate (*https://support.google.com/accounts/answer/6386856*), but this feature does not include browsing or location information.

Family Link accounts for children can "graduate" into regular accounts, at which point they are told about their options and given information to help them make appropriate choices about data use, including ads. Even if a user enables personalized ads, we take steps to prevent data from before the user's "graduation" from being used for advertising purposes.

Question 5. It is my understanding the Google allows advertisers to target users who are experiencing "important life milestones, like graduating from college or get-

ting married." What user data does Google use to infer life milestones and family status? Does Google provide the user with a way to opt-out of this data collection?

Answer. Yes, certain demographic topics like these can be inferred based on activity, for instance based on a user's searching for wedding dresses or caterers. These topics will be visible in a couple ways:

- A user can click or tap on the Why This Ad link in or near the ads we show, which explain what criteria was used to select the specific ad.
- The Ad Settings tool, also available via Why This Ad or the Google Account, shows all the topics, advertisers, or demographics associated with the user's account, and allows the user to delete their profile and opt out of personalized ads, including these demographic topics.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO KEITH ENRIGHT

Question 1. Positive Aspects of State Laws/GDPR: Your company has called for a national privacy framework in order to avoid a patchwork of state laws which you have to comply with as your data travels across state lines. From an international perspective, Europe has GDPR. You have operations around the country, and some around the globe and have seen firsthand how these laws are being implemented.

Are there any states that you believe have the right framework, or aspects, in place?

Answer. All fifty states have enacted security breach notification statutes that can be useful lodestars for Congress as it considers legislation that would establish a national security breach notification regime. While the statutory triggers for notification vary from state to state, these laws share the common objective of ensuring consumers are notified in the event that their personal information is accessed or acquired by unauthorized parties. Importantly, many states set notification thresholds to guard against over-notification (*e.g.,* when certain types of personal information are at issue).

Many states have played important roles in modernizing government access laws in light of technological innovation, as well as the reasonable and evolving expectations of privacy that users have in their electronic communications. In 2016, for example, California enacted the California Electronic Communications Privacy Act (CalECPA), which Google supported. CalECPA generally requires governmental entities to obtain a search warrant for electronic data, including the contents of electronic communications, location information, data that relates to the content of electronic communications, and information on electronic devices.

Question 2. Can you point to an aspect of the California law that you believe is reasonable and should be emulated on the national level?

Answer. With regard to the recently enacted California Consumer Privacy Act (CCPA), we support the goals of the law, including increased transparency and user control, but share the concerns that many have expressed about how the law is drafted and its impacts on businesses and consumers. In particular, we hope that the law can be clarified to make it easier for consumers to understand and exercise their rights, and ensure that companies of all sizes and sectors can comply and continue to offer innovative products and services consumers rely on. At the same time, we believe the CCPA does not go far enough in codifying the rights and obligations included in consensus frameworks such as the Fair Information Practices Principles (FIPPs), OECD Privacy Principles, APEC Privacy Framework, and even Europe's General Data Protection Regulation (GDPR). We recently put forward principles for a responsible data framework (*https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf*), based on the aforementioned frameworks, and our 20 years of experience offering services that depend on information, privacy protections, and user trust.

Question 3. Nevada passed a privacy notice law during the 2017 session, how is your company doing in complying with this?

Answer. Google's Privacy Policy (*https://policies.google.com/privacy*) identifies the information we collect, why we collect it, and how users can update, manage, export, and delete their information.

We believe we exceed the requirements of the Nevada privacy law. We realize privacy policies aren't user's first choice of reading material, but we worked to make ours best-in-class, with illustrations, videos and other interactive content designed to convey key concepts and choices.

Question 4. What difficulties have your companies faced when developing more transparent privacy policies?

Answer. We value being transparent with our users about how and why we use data to operate our business. Making this information available is critical to building and maintaining user trust, and specifically helps our users make important decisions about their privacy. One challenge we have encountered is how to ensure users have the information they need, without overwhelming them with extraneous details. We are constantly refining this balance based on feedback from our users.

We recently updated our privacy policy to incorporate some of the insights we have gained. While we don't solely rely on the privacy policy to educate users, we still want to make our policies understandable and accessible to users who spend the time to review them as well as being full and complete statements of our data practices for experts and regulators to hold us accountable. We try to meet both needs, via clear headings, easy navigation, overlays and examples, and explanatory videos.

We also regularly conduct surveys and interviews with users to inform our approach and ensure we strike this balance effectively.

In addition, we try to really help users understand, in real time and in context as they use our services. We gave some examples in my testimony, and just last week added new transparency in our flagship product, Search, that shows users exactly how their data is being used to improve their search results, along with direct access to controls (*https://www.blog.google/technology/safety-security/making-it-easier-control-your-data-directly-google-products/*).

Question 5. What part(s) of the GDPR should we look to emulate in the U.S.?

Answer. We support thoughtful privacy legislation that both protects consumers and encourages businesses to continue innovating. While we don't agree with everything in the GDPR, and indeed there are aspects of it that reflect specific European standards that aren't globally applicable, the Regulation does rest on global fair information practice principles that also inform our model framework. For example, the GDPR includes requirements of transparency, user control, data quality, and security, to name a few.

In particular, we would point to the GDPR's concept of a "data processor" versus "data controller" as a useful way to distinguish providers of general consumer services from enterprise services that act as "vendors" for others, without independent rights to process data on their own behalf. This concept is a helpful way to allow for the efficient use of vetted, qualified vendors with minimal additional compliance costs, which is particularly important for smaller entities. Processors can look to the controller to meet certain obligations under the law, including transparency, control, and access, but processors must still meet basic programmatic and security responsibilities.

We also support the GDPR's notion of "legitimate interests" as a positive way to permit standard or typical data uses that are consistent with individuals' interests while reserving express consent to those situations where users really need to pause and consider their choice.

Question 6. State Attorneys General: I understand the utility of having a national framework given how difficult it would be to develop 50 different frameworks based on state law. At the same time, we want to ensure that states play a role in protecting the privacy of their residents.

What should, in your view, be the role of State AGs in enforcing privacy standards?

Answer. We believe State Attorneys General have been effective in enforcing privacy and security issues individually and collectively using a range of privacy and data security laws. They are also the primary enforcers of state Unfair and Deceptive Acts and Practices (UDAP) laws which enable them to obtain civil penalties, injunctive relief, and attorneys fees and costs.

Question 7. Law Enforcement: I believe our law enforcement officials should have a mechanism to obtain the data they need for legitimate investigations. At the same time we need to strike the right balance between keeping our country and communities safe while protecting individuals' civil rights and privacy. Your company has access to many of the personal and intimate choices of millions of your customers, data and records that paint the picture of the everyday lives of millions of American families.

How do you believe a national privacy framework could seek to strike the right balance?

Answer. People now use Internet services in ways that broadly reflect their reasonable expectations of privacy. E-mails, electronic documents, photos, search queries, and other private communications should have the same strong privacy protections as documents stored on a hard drive or letters filed in a drawer.

The Electronic Communications Privacy Act (ECPA), enacted in 1986, makes distinctions that simply don't reflect reasonable expectations of privacy. For example, ECPA's privacy protections for an e-mail depend on how old it is or whether it's been opened.

We have long supported passage of the E-mail Privacy Act, which would require governmental entities to obtain a warrant in order to compel a service provider to disclose the content of a user's electronic communications. The E-mail Privacy Act unanimously passed the House in 2016 and passed by voice vote in 2017 and 2018 but has yet to become law.

Government access laws should reflect reasonable expectations of privacy and the increasing importance of online services to our daily lives. Measures like the E-mail Privacy Act demonstrate that this goal can be achieved while protecting important law enforcement interests.

Question 8. Privacy Enhancing Technology: There are many technologies that actually enhance users' privacy: Encryption, anti-virus, cybersecurity technologies are all examples of this. I think this is a portion of the privacy debate that sometimes gets looked over, but one we should consider as we look at privacy legislation.

Can you summarize some of the privacy enhancing technology used at your company?

Answer. We continually research, develop, and implement advanced technical privacy techniques in our products. Some examples include:

- Federated learning: this method can train machine learning models using data that never leaves a user's device. This technology is used to train smart features in Gboard for Android and on Google Pixel devices. Federated learning can also utilize a user's data to enable personalized models on-device.
- Secure aggregation protocol: Provides strong cryptographic privacy for individual user updates in a federated learning model, averaging only updates from large groups of participants. One example of this technique enables researchers to learn the quantity of overlapping users between different data sets (two or more) without learning other information about the data, including the identities of those who may be included. It enables us to understand some similarities between datasets without sharing additional information. Applying this at scale, as we do, is a novel use of the concept. There are also public-interest applications for this technology—for example, determining how many people visit both a homeless shelter and the VA but not revealing to either institution who those people are.
- Differential Privacy: Differential Privacy protects the presence or absence of an individual in a dataset, protecting users privacy with a high degree of mathematical guarantee. At Google we make use of Differential Privacy for a variety of use-cases. For example, we use the central differential privacy model to produce differentially private results when querying data Google holds as part of our own products (*e.g.,* Gmail). We also use differential privacy to ensure that even frequently-queried datasets have a high degree of privacy protection. We are continuously expanding on our differential privacy work in practice, and are regularly producing research on this and related topics.
- Homomorphic Encryption: Homomorphic encryption allows a data processor (such as a cloud service) to operate on data that remains encrypted. For example, it enables researchers to query a medical database for information about some disease without revealing what disease they're searching to the owner of the database. Google uses homomorphic encryption as a component of Secure Multiparty Computation and has published an open-source homomorphic encryption library which enables broader use of this technology.
- Measuring unintended neural network memorization & extracting secrets: Presents an easily applicable exposure metric for assessing unintended machine learning model memorization of secret data. This technique can be used during model development and during model maintenance (*e.g.,* in regression tests), and findings from this research was recently used during the development of Smart Compose in Gmail.

We appreciate your interest here and would welcome the opportunity to further discuss these and other advanced techniques with you and your staff.

Question 9. Do you believe the Federal Government could assist in either funding the development of similar technologies or establishing a framework for companies to implement them into their data processing?

Answer. Yes. We believe the Federal Government has an important role to play in enabling the development of privacy and security enhancing technologies.

We encourage the Federal Government to continue providing funding for the research and development of products, services, and techniques that improve privacy and security protection. Basic research remains cost intensive and educational institutions and research organizations need sustained funding to make the critical long-term investments that lead to new and improved ways to protect privacy and security. However, in its support, the government should not only focus on the products and services that consumers see as an end-result, but also on expanding the types of tools and training available to practitioners. For example, techniques for internal data management and expanded availability of ethics training in schools can promote better outcomes for consumers.

The government should also consider establishing local centers of excellence for privacy and security research and applications, perform privacy and security research at government labs and agencies, create frameworks and mechanisms to facilitate public-private sector collaboration, and explore incentives for researchers who receive public funding to explore priority areas of research. Google has long supported open-source research, and we encourage open access to publicly funded research.

In addition the U.S. Government should leverage its convening power to disseminate best practices to ensure that every organization that processes personal data, including the government itself, can keep abreast of and implement the state of the art. Publications, public events, technical workshops, digital literacy programs, and advisory committees, are potential ways the government could achieve this goal.

Question 10. Small Business: As we talk about a national framework, one of the most important things to keep in mind is how we work with small business. Your company has the ability to maintain cybersecurity and compliance teams that make it easier for your companies to work with any potential law we pass.

Can you discuss how your companies might be working with, or aiding, small businesses with their privacy and data needs?

Answer. We agree that it is important to keep small businesses front of mind. In general, we work with our enterprise and advertising customers to help them meet comply with applicable laws, including by providing products that enable them to meet their privacy obligations. (See *e.g., https://privacy.google.com/businesses/compliance/*) We sit on the board of—and have been key supporters of—the National Cyber Security Alliance. Their outreach and trainings include webinars and in-person workshops for individuals and small- and medium-businesses on cybersecurity, which is an essential component of data privacy. We have many small- and medium-business clients of our G Suite and Google Cloud products, which offer many built in security and privacy features.

In addition, we offer free and publicly available products such as Safe Browsing (*https://safebrowsing.google.com/*) for developers, webmasters, and other companies to use in their applications and browsers. Safe Browsing currently protects over three billion devices every day. Our tools such as Search Console and Developer Console enable businesses of all size and capabilities to understand quickly and easily how their site or app is performing and to diagnose and correct security or privacy issues (*e.g.,* if their site were hacked and hosting malware, unbeknownst to them).

Improving privacy and security across the Internet ecosystem is a team effort, and we want others to benefit from the investments we have made. That is why we actively share research on engineering techniques and user experience through open publication and participation in conferences and other public events. We also aim to raise standards across the ecosystem by publishing information and guidance on such security-and privacy-enhancing techniques as e-mail encryption in transit (see our Safery E-mail work at *https://transparencyreport.google.com/safer-e-mail/overview*), as well as the use of HTTPS on the web to secure connections to websites (*https://transparencyreport.google.com/https/overview*).

To facilitate portability more broadly, Google led the development of the Data Transfer Project (*https://datatransferproject.dev/*), an open-source platform enables individuals to move a copy of their data directly from one account to another, without downloading and reuploading. By collaborating on the code, and establishing a shored understanding of the fundamentals, we hope to make it easier for all service providers to provide users the ability to directly transfer their data into and out of the provider of their choice, with strong privacy and security measures such as transparency and data minimization.

Question 11. Also, can you provide your thoughts on how a Federal framework would best take the challenges and opportunities of small businesses into account?

Answer. A Federal framework should optimize for accountability, risk management, and flexibility to best take into account the resource constraints of small businesses.

Lawmakers and regulators should set baseline requirements, but enable flexibility in how to meet those requirements. Accountability can and should come in many forms, and a Federal framework should encourage diverse and innovative approaches to compliance. We believe that small businesses can achieve the same protections and accountability without building a privacy program with the same scope and scale that larger, more established companies like Google operate.

A Federal framework should take care to avoid overly prescriptive requirements, especially those without commensurate consumer protections, which can disadvantage small businesses. An example of this potential impact on small business is the requirement in the recently enacted California Consumer Privacy Act (CCPA) that user privacy notices and controls be provided in exactly the manner and location prescribed in the statute, as well as the requirement for every business to maintain a toll-free number to field user requests. Ideally, the law should allow the principles of transparency and control to be met differently by different organizations.

Question 12. Data Protection Officers: As you all 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 company's perspective on this requirement?

Answer. As expressed in our privacy framework proposal, the guiding principles here should be accountability and protecting individuals and communities from harm. Privacy programs, including appointment of a DPO or similar role, should be aimed at minimizing risk of harm to users and demonstrating that the organization is accountable for meeting its legal commitments and promises. The DPO is one mechanism to achieve this goal, but we would encourage laws and regulations to not be inflexible as to what specific structure is best for achieving these goals. We should encourage innovation in compliance just as we do in products and services.

Question 13. Data Minimization: One component of the GDPR is a concept known as "data minimization." This principle states that data processing should only use as much data as is required to successfully accomplish a given task and data collected for one purpose cannot be repurposed without further consent. The idea behind this is both to ensure that users are comfortable that their data is only being used for the purposes which enhance the experience and also help limit the impact of any data breaches. It seems like there may be challenges to implementing something this broad, especially as it is laid out in the GDPR, but it nonetheless feels like something that should be explored as part of our conversation here in the United States.

What is your company's perspective on this requirement?

Answer. As expressed in our framework for responsible data protection (*https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf*), we believe that reasonable limitations should be placed on the manner and means of collecting, using, and disclosing personal information. We believe that collection and use of personal information can create beneficial and innovative services, within a framework of appropriate limits to the collection, use, and disclosure of personal information to ensure processing occurs in a manner compatible with individuals' interests and social benefits and minimizes the risk of harm based on the use of personal information.

Our understanding of the GDPR's principle is similar to this: to limit data processing to "what is necessary in relation to the purposes for which they are processed." While we do not yet know precisely how this will be applied, we concur with the general sentiment that beneficial use of data should be encouraged, yet data uses should be circumscribed to limit risk of harm to individuals.

Question 14. 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.

Do you build your own data centers or contract with another entity?

Answer. Google owns and operates several of its own data centers. We place some of our production infrastructure in data center facilities owned and operated by third-party providers.

Question 15. What steps do you take to secure these centers?

Answer. We take security very seriously, particularly at our data centers. We keep data secure by employing many security features. For example,

- Access to data centers is limited to only a very small fraction of Google employees.
- We use multiple physical security layers to protect our data center floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems.
- Google additionally hosts some servers in third-party data centers, where we ensure that there are Google-controlled physical security measures on top of the security layers provided by the data center operator. For example, in such sites we may operate independent biometric identification systems, cameras, and metal detectors.
- We distribute all data across many computers in different locations. We then chunk and replicate the data over multiple systems to avoid a single point of failure. We randomly name these data chunks as an extra measure of security, making them unreadable to the human eye. Our servers automatically backup critical data so it is always available to our users, even when incidents happen, such as if a user's device is stolen.
- We rigorously track the location and status of each hard drive in our data centers. We destroy hard drives that have reached the end of their lives in a thorough, multi-step process to prevent access to the data.
- We employ a full-time Information Security Team that maintains the company's perimeter defense systems, develops security review processes, and builds our customized security infrastructure. It also plays a key role in developing and implementing Google's security policies and standards. At the data centers themselves, we have access controls, guards, video surveillance, and perimeter fencing to physically protect the sites at all times.

More information about the steps we take to secure our data centers in our white paper available at *https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf*)

Question 16. How often do you review your physical data security standards at your data centers?

Answer. Google regularly tests and audits the security measures at our data centers to confirm the policies and processes we have in place are working as intended. In addition, our products and infrastructure regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards such as $ISO_2$7001 (see current certifications at *https://cloud.google.com/security/compliance/iso-27001/*).

Question 17. Data Use: Does Google scan content stored in a user/consumer "Google Docs" or "Google Drive" to infer user activities and interests?

Answer. Our automated systems analyze content, including that stored in Google Docs and Google Drive, to provide users personally relevant product features, such as customized search results, and spam and malware detection.

Question 18. Does Google use this information for advertising purposes?

Answer. Google does not use content in these services to create any advertising profiles or to serve personalized ads.

Question 19. When a user turns off Ads, does Google stop tracking the user's interests?

Answer. Users cannot generally turn off ads in Google's free services. Users can disable personalized ads, which will stop the use of the user's information or activity to form an ad profile or to personalize ads.

Question 20. Does the Google "Takeout" function contain all the data that Google has collected on each user?

Answer. Our goal is to enable users to download or export their data from the Google products they use. What is now known as Google's "Download Your Data" is limited to users we are able to authenticate and safely and securely show their data. Users who are not signed-in have other ways to control their data we collect about their use of our services and devices.

There are other practical limitations as well: We don't want to overwhelm users with detail, so might show a single event (*e.g.,* a search query), when we log several interactions (*e.g.,* the initial page load, the query, each page of results). Some data is stored only on a temporary basis—hours or days—before being deleted. Finally, some activity is not yet technically possible to download, because of changes to in-

frastructure, new products that have been released, or other technical limitations. We aim to reduce this category of information over time.

Question 21. China: Can you give specific examples of ways in which Google has applied its privacy-related Artificial Intelligence (AI) principles to its AI research in China?

Answer. Consistent with our AI principles, all of our work undergoes rigorous privacy and other reviews. Google has AI research teams in many locations around the world—including Mountain View, Seattle, New York, Toronto, Zurich, Paris, London, Amsterdam, Beijing, Tokyo, Tel Aviv, and Accra—building on local talent and the strength of academic institutions in the region. Google's AI principles are meant to guide our work everywhere. Our AI work in Beijing consists of a team of researchers undertaking basic questions in algorithm development and applications for health, and we understand many other U.S. companies are engaging in similar or more extensive work in the region.

Question 22. How does Google ensure its AI center achieves its research goals while adhering to AI Principle 5 on incorporating privacy safeguards into all AI technologies?

Answer. We are focusing on academic exchange with some of the world's top AI researchers—through this center, as well as at research centers in countries around the globe (for example ETH Zurich in Switzerland, Stanford's AI lab in the U.S., the Vector Institute at the University of Toronto that Google co-founded, and the Montreal MILA institute). As noted in response to the question above, all of the AI work we do—from basic research to implementation in products—goes through rigorous privacy and other reviews to ensure alignment with our AI principles. You can read more about the specific work we are doing in our Responsible AI Practices on Privacy, which outlines all of our work and recommendations to date.

Question 23. What precedent would adopting privacy rules required by a non-democratic government, like China and others, set for your company's operations in other non-democratic governments?

Answer. Google currently serves users in countries with very different histories, political institutions, and cultural sensitivities—and hence with different approaches to privacy. We are required to comply with the laws of the jurisdictions in which we operate. Our privacy program and our privacy rules are designed to meet our own principles and standards, as well as relevant laws.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO DAMIEN KIERAN

Question 1. Efforts to draft meaningful Federal legislation on consumer data privacy will heavily rely upon determinations of what types of personally identifiable data are classified as "sensitive" and what are not. While some have suggested that expanded FTC rulemaking authority is necessary to flexibly account for new types of data sets coming from innovative technologies, I have concerns that excessive rulemaking authority could lead to frequent reclassifications of the types of data with ensuing liability adjustments. Do you have suggestions on how to best identify "sensitive" personally identifiable information?

Answer. Twitter believes it is important to strive for global consistency in the definition of these important terms to the extent possible. To that end, the European General Data Protection Regulation (GDPR) offers definitions for personal data and sensitive personal data that we believe are good starting points for defining these terms in the United States. GDPR defines personal data as any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. The GDPR indicates "sensitive" personal data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed solely to identify a human being, health-related data, and data concerning a person's sex life or sexual orientation. Importantly, different information could be considered sensitive in different circumstances, and regulations should have the flexibility to consider context.

Question 2. NTIA issued a request for comment on ways to advance consumer privacy without harming prosperity and innovation. I commend the administration for their attention to this important issue. The "High Level Goals for Federal Action" that NTIA is seeking comments for includes inter-operability and the development of a regulatory landscape that is consistent with the international norms and frame-

works in which the U.S. participates. How do you foresee Federal legislation affecting cross-border data flows?

Answer. Twitter's services are primarily designed to help people share information around the world instantly. We have offices, partners, and service providers around the world that help to deliver our services.

User information, which we receive when an individual uses our services, may be transferred to and stored in the United States and other countries where we operate, including through our offices, partners, and service providers.. We rely on various legal mechanisms to lawfully transfer personal data around the world.

To effectively provide our services to people around the world, it is vital that Twitter be able to transfer data across borders. Thus, Twitter agrees with NTIA's assertion that the growth and advancement of the Internet-enabled economy depends on personal information moving seamlessly across borders. It is therefore critical that any Federal legislation be consistent with international norms and frameworks in which the U.S. participates.

Question 3. Also included in NTIA's request for comments, how should the U.S. government encourage more research and development of products and services that improve privacy protection?

Answer. Twitter agrees with NTIA's recommendation that the U.S. Government should encourage more research into, and development of, products and services that improve privacy protections. Areas that should be considered for research and development of products and services that improve privacy protection potentially include processes and mechanisms for obtaining informed consent, mechanisms to improve the utility of privacy policies, studies on the efficacy of privacy policies, tools to enable the portability and interoperability of data, strong encryption, and effective anonymization techniques. Twitter believes that fostering research and development in these areas can be achieved if an overarching, industry-neutral Federal privacy legislation is created. Properly structured privacy legislation has the potential to incentivize healthy data protection practices over time, which in turn will result in investments in these areas to both reduce risk and maintain user trust.

Question 4. 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. It is too early to understand the full impact of the right to be forgotten with respect to data ingested by algorithms and how regulators may interpret this language in the GDPR. At Twitter we believe individuals should have meaningful control over their data. We provide individuals with a variety of meaningful controls over they data we receive about them. For example, they can access or rectify their personal data at any time and can also deactivate their account. Where applicable we also provide users with tools to object, restrict, or withdraw consent. Lastly, we make the data individuals share through our services portable.

Question 5. 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. Please see above in response to Question 4. With respect to ownerships of outputs of algorithms, it will depend on the circumstances and the type of information that has been created.

Question 6. Since companies often use aggregated data outputs to study and improve their existing algorithms, services, and products, what impacts do you expect these vague GDPR requirements to have on companies' abilities to innovate?

Answer. Twitter is still working to assess the impacts of GDPR implementation on our business and practices. We do believe, however, that care should be taken in crafting legislation to guard against language that overly restricts the ability of companies to utilize non-personalized, aggregated data for things like improving services for customers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELLEY MOORE CAPITO TO DAMIEN KIERAN

Question 1. According to a study by Pew Research, only 38 percent of consumers know how to limit what information they give online. Consider me among those consumers who do not know what is being collected and how to keep my information

to myself. Even with privacy settings and assurances that my data is not being collected and used without my consent, I still have concerns.

I believe the root of this issue is transparency and consumer confidence. What are your companies doing to increase the transparency when it comes to the type of data you collect?

Answer. Twitter designs its products to be as intuitive as possible for users to understand what data is being collected, how it is used, and when it is shared. To create a Twitter account, individuals need not provide their real names, phone number, or primary e-mail address. Most users come to Twitter with the intention and expectation that their profiles, Tweets, and engagements will be public and shared to a global audience. In addition, to address the details of how our service works, we have an easily accessible privacy policy, which has been designed to explain what data we collect, how it is used, and when it is shared. Earlier this year we undertook a thorough revision of our Privacy Policy in an effort to make it easier to understand for consumers. It is a single document, not spread out over multiple web pages. It contains animations, graphics, and innovative uses of technology in an effort to transparently explain what data we collect, how it is used, and when it is shared. We plan to keep improving how we convey this information.

In addition, when individuals on Twitter log into their accounts, they have immediate access to a range of tools and account settings to access, correct, limit, delete or modify the personal data provided to Twitter and associated with the account, including public or private settings, marketing preferences, and applications that can access their accounts. These data settings can be used to better personalize the individual's use of Twitter and allow him or her the opportunity to make informed choices about whether Twitter collects certain data, how it is used, and how it is shared. For example, individuals can change the personalization and data settings for their Twitter account, including:

- Whether interest-based advertisements are shown to an individual on and off the Twitter platform;
- How Twitter personalizes an individual's experience across devices;
- Whether Twitter collects and uses an individual's precise location;
- Whether Twitter personalizes their experience based on places they have been; and
- Whether Twitter keeps track of the websites where an individual sees Twitter content.

An individual on Twitter can disable all personalization and data setting features with a single master setting prominently located at the top of the screen. Twitter also provides a toolset called Your Twitter Data. Your Twitter Data tools provide individuals accessible insights into the type of data stored by Twitter, such as username, e-mail address, and phone numbers associated with the account and account creation details. The birthdays and locations of individuals are also shown in the tool if they have previously been provided to Twitter.

Individuals using the Your Twitter Data tool can also see and modify certain information that Twitter has inferred about the account and device such as gender, age range, languages, and interests. People on Twitter can review inference information, advertisers who have included them in tailored audiences, and demographic and interest data from external advertising partners. The Your Twitter Data tool also allows people with a Twitter account to download a copy of their relevant data from Twitter. We recently updated the download feature of the Your Twitter Data tool to include additional information. Since that update on May 25, 2018, we have seen approximately 85,4587 people around the world use the tool to download 909.9 terabytes of data.

There is a version of this tool available to individuals who do not have a Twitter account, or for those logged out of their account.

Question 2. What difficulties have your companies faced when developing more transparent privacy policies?

Answer. Privacy policies must convey complicated legal and technical constructs in as simple a format as possible. Developing a privacy policy that is equally and easily digestible for a wide and global user base is challenging. One way we work to overcome this challenge is to work with people who are not experts or lawyers to review drafts of our privacy policy and identify areas that were complicated for them to understand. With that in mind, we reworked drafts of our policy to account for these concerns and used user-friendly graphics and intelligent uses of technology to make the latest version of our Privacy Policy more relatable and understandable. The result is a single document that is not spread out over multiple web pages and that includes call outs, graphics, and animations. We believe, however, that it is im-

portant to learn from the people who use our services to keep our Privacy Policy as transparent and easy to understand as possible. Thus, our work on transparency will continue and evolve as we learn.

Question 3. West Virginia has a high elderly population that is rapidly increasing as baby boomers retire. I am positive that a lot of my elderly constituents are among those individuals who do not know how to limit their online information.

What are some of the measures your companies are doing to teach consumers—and specifically older consumers—about what data they share on your platforms?

Answer. Please see responses to Questions 1 and 2. We crafted our Privacy Policy to be understood by our broad user base. It contains animations, graphics, and innovative uses of technology in an effort to transparently explain what data we collect, how it is used, and when it is shared. We plan to keep improving how we convey this information, and we will always lead with transparency and openness.

Question 4. I know advertising through data collection has a monetary value, and appreciate the business model, however, I find it hard to know what is being collected and how I can keep my information to myself. Even with privacy settings and assurances my data is not being used without my consent, I still have concerns.

Please explain how your business model allows both data to be used to make suggested recommended purchases on your site? As well as how you use that data to target ads to consumers? And how do you do that while protecting personal data?

Answer. Twitter doesn't directly sell any goods or services on our platform. Twitter's mission is to serve the public conversation. To enable that mission, we enable people to see the most relevant content to them, whether organic content or advertising content. Ensuring that people see the most relevant content for them is an important feature of our service. Thus, the information we rely on to power our advertising experience is generally the same as the information we rely on to enable people to see the most relevant content for them.

Advertising revenue allows us to support and improve our services. We use the information described in our Privacy Policy to help make our advertising more relevant to our users, to measure its effectiveness, and to help recognize devices for those individuals on our platform to serve ads on and off of Twitter.

In addition, Twitter adheres to the Digital Advertising Alliance (DAA) Self-Regulatory Principles for Online Behavioral Advertising (also referred to as "interest-based advertising") and respects the DAA's consumer choice tool for you to opt out of interest-based advertising. If an individual does not want Twitter to show interest-based ads on and off of Twitter, there are ways to turn off this feature. In addition, our ads policies prohibit advertisers from targeting ads based on categories that we consider sensitive or are prohibited by law, such as race, religion, politics, sex life, or health.

Question 5. How can Congress ensure that data collected is used responsibly without shutting down the collection of data completely?

Answer. We believe that the time is right for industry, civil society, and government to work together to develop a robust privacy framework that protects individuals' rights by ensuring transparency and accountability while preserving the freedom to innovate. We provide meaningful data protection policies for consumers and respect our users' data. We also believe that our accountability measures, including appointment of a Data Protection Officer to assess compliance and performing data protection impact assessments to ensure collection and processing is consistent with user expectations, are all ways to help ensure responsible handling of data collection and use.

Response to Written Questions Submitted by Hon. Todd Young to Damien Kieran

Question 1. GDPR establishes a right of data portability, which some believe is key to driving new innovation and competition within the emerging data ecosystem. Others are concerned that data portability rights, depending on how crafted, could further entrench incumbent companies.

What questions should policymakers be asking in developing data portability rights?

Answer. At Twitter, we feel strongly that portability and interoperability are central to innovation on the Internet. We believe that more frictionless, individually-driven forms of data transfer between online platforms and services will result in an innovative, creative, and people-first online experience for all. Making it easier for users to choose among services also facilitates competition, empowering everyone to try new services and choose the offering that best suits their individual needs.

This facilitative and collaborative spirit of openness is the principled bedrock of our free and open internet. It is a principle we at Twitter are dedicated to furthering. That is why Twitter, alongside Google, Microsoft, and Facebook, is leading the Data Transfer Project, an open source initiative aiming to empower any company to create tools that enable people to freely move their information across the web without barriers. For more information, a white paper we co-authored with our Data Transfer Project partners may be found here: https://datatransferproject.dev/dtp-overview.pdf

Question 2. What improvements would you make, if any, to Art. 20 of GDPR, which addresses the right to data portability?

Answer. Twitter believes that Article 20 provides a good starting point to ensure that data is freely and easily accessible by people.

Question 3. How best can data portability rights be crafted to create new competition, but not further entrench incumbent companies?

Answer. In a white paper we co-authored with our Data Transfer Project partners (available at: https://datatransferproject.dev/dtp-overview.pdf), we articulate a series of principles around interoperability and portability of data that could promote user choice and encourage responsible product development in order to maximize the benefits to users and mitigate the potential drawbacks.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO DAMIEN KIERAN

Question 1. In general we have been exploring the idea of opt in frameworks to keep consumers informed about what their data is being used for. However, we know from recent history that there are some uses of data that should never be permitted—like the leveraging personal data to interfere with election processes. How could we design an opt in framework that is meaningful to consumers, doesn't desensitize them to important decisions about privacy and makes sure they consent only to lawful uses of their data?

Answer. At Twitter, we believe in the principle of informed consent and believe that informed consent can be achieved in a number of ways. While opt-in consents have a purpose and a place, we believe that blanket opt-in consent requirements should be avoided for a number of reasons. For example, blanket opt-in consents would make it operationally and technically challenging to serve a person with an onboarding experience in their home language based on their IP address if a service has to get consent before processing the IP address. Providing people with information about how this works, and the ability to modify or opt-out of such processing would, however, meet the objective of informed consent. Thus, while informed consent should always be the goal, the mechanisms for achieving informed consent should be flexible based on—among other factors—the service, the type and sensitivity of information for which consent is sought, what is to be done with the information, and when during the use of the service consent is needed.

Question 2. Short of regulation, what more can you and your colleagues and competitors do to restore and maintain our and our constituents' trust that you won't continue to collect more data than consumer understand, use it in ways they never imagined, and then fail to protect the data from unauthorized use and access?

Answer. Twitter's purpose is to serve the public conversation. We serve our global audience by focusing on the people who use our service, and we put them first in every step we take. We are aware that many people around the world use Twitter like a "town square" to publicly, openly, and freely exchange ideas. We must be a trusted and healthy place in order for this exchange of ideas and information to continue.

To ensure such trust, the privacy of the people who use our service is of paramount importance to Twitter. We believe privacy is a fundamental right, not a privilege. Privacy is part of Twitter's DNA. Since Twitter's creation over a decade ago, we have offered a range of ways for people to control their experience on Twitter, from creating pseudonymous accounts to letting people control who sees their Tweets, in addition to a wide array of granular privacy controls. This deliberate design has enhanced privacy protections and choices for the people who use Twitter.

That same philosophy guides how we work to protect the data people share with Twitter. Twitter empowers the people who use our services to make informed decisions about the data they share with us. We believe individuals should know, and have meaningful control over, what data is being collected about them, how it is used, and when it is shared. We are constantly looking for ways build trust and to be more transparent with our users, including through regularly iterating our own

privacy policy. This ongoing work enables us to receive and act upon feedback, keeping us accountable to our customers while providing them with the information they need and deserve.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO DAMIEN KIERAN

Question 1. State Preemption: Several public interest organizations have written the Committee in advance of the hearing expressing their deep concerns about state preemption. As the ACLU noted, it has often been the states—not the Federal Government—that have acted in a timely and important way to protect consumer interests.

Please provide to me a set of recommendations for how to improve the California Consumer Privacy Act and the GDPR.

Answer. Twitter believes that both the California Consumer Privacy Act and the GDPR provide good foundations when considering Federal legislation. The GDPR was crafted over a number of years, and while it is EU-centric and sensitive to EU concerns, the objectives of the GDPR—to ensure the protection of privacy as a fundamental right—is borne out in the carefully considered language it contains. That said, there are areas where Twitter believes adjustments should be made to the GDPR as its concepts are considered by lawmakers contemplating potential Federal legislation in the United States. In addition, while Twitter believes that people should be able to erase the information they provide to a service—and Twitter provides people the ability to erase their data—we believe that the commonly titled 'right to be forgotten' in the GDPR is inconsistent with American concepts and traditions around free speech, journalism, and "right to know" consumer benefits.

Question 2. Privacy by Design: Between the six of your companies, you have access to an overwhelming amount private information about nearly everyone in the United States. AT&T and Charter have access to the browsing history of your customers. A Princeton study found that Google collects visitor data from 70 percent of websites—including from Twitter, a competitor. It's hard to imagine what your companies don't know.

Would you commit to privacy-by-design—limiting collection of data and deleting data when it is no longer useful to your customers?

Answer. Twitter believes that privacy-by-design is key to accountable data protection practices and we are already working to ensure these concepts are embedded in they way our teams work at Twitter. Twitter believes that we should only collect and use personal data to provide the best possible services that individuals on our platform deserve and expect, including by limiting what personal data we collect at the outset by giving users more choice about what we collect, as well as by ensuring that we have appropriate retention periods for personal data.

Question 3. What specific steps do you plan to take to limit your own use of customer data? Can you provide examples where you deleted or stopped collecting data to protect privacy?

Answer. At Twitter, our work is guided by the belief that we should only collect and use personal data to provide the best possible services that our users deserve and expect. Twitter empowers the people who use our services to make informed decisions about the data they share with us. We believe individuals should know, and have meaningful control over, what data is being collected about them, how it is used, and when it is shared.

Question 4. Privacy by design is fundamental to the GDPR. What specific changes have you made to your products to come into compliance to the GDPR's privacy-by-design requirements?

Answer. Protecting and defending user privacy is at the heart of our work. From permitting user anonymity and pseudonymity, to offering meaningful privacy and security controls, and our overall commitment to transparency, these are foundational principles built into the core DNA of our company. In preparing for GDPR, we formed a cross-functional team made up of senior team members from across Twitter to make sure we are not only working towards GDPR compliance as an end in itself, but in a way that evolves our principles and overarching mission as a company. Our teams have been working on a consistent basis to ensure privacy is taken into account across our core product, policy, and operations from the earliest stage in the life cycle of a product, feature, or project. For example, one way in which we ensure privacy-by-design is to have teams do an early privacy review of a project to determine at the earliest stages whether the project may need a formal data protection impact assessment. This helps to ensure that privacy-by-design

is embedded in the way teams are working at Twitter. Our goal, as ever, is to meet our commitments to our users and to provide an industry-leading level of transparency and user control.

Question 5. FTC Rulemaking—In most of your remarks, you discuss the challenges of regulating evolving technologies and economies. It would seem to me that this requires a Federal agency that is responsive to technology changes.

Would you support the FTC having rulemaking authority to provide clarity, to address potential harms, and to ensure rules match technology changes? What sorts of areas should this cover?

Answer. Twitter believes that the FTC should be granted the resources and authority it requires to fulfill its important mandate and provide more clear, specific guidelines. As part of pre-emptive Federal legislation, Twitter believes the FTC should be able to provide the appropriate guidance to ensure the underlying goals of the Federal legislation are achieved.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO DAMIEN KIERAN

Question 1. Unsurprisingly, none of your testimony speaks about potential increased penalties for a new privacy framework. The current penalty regime seems not to change corporate behavior—as we repeatedly have seen. In your opinion, are civil penalties an effective mechanism to push companies to follow the law? If not, what mechanisms would be effective?

Answer. Twitter makes every effort to comply with U.S. state and Federal laws, regardless of the penalties of non-compliance. While penalties are a part of ensuring accountability there are number of ways including appointment of individuals like Data Protection Officers or requiring impact assessments that also drive accountability. Thus, increased penalties are not the only lever to ensure compliance with applicable laws.

Question 2. Mr. Kieran, one of Twitter's subsidiaries, MoPub, is a mobile advertising network. As you know, we need the entire mobile ecosystem to support COPPA. As such, MoPub and other advertising networks have a place in building technologies that help mobile developers comply with COPPA. Why did MoPub decide not to support COPPA compliance for its customers?

Answer. MoPub, a division of Twitter and Twitter International Company, provides advertising technology services that allow publishers of mobile applications to show ads in their apps, and for advertisers to reach audiences that may be interested in their products and services. MoPub's policies clearly prohibit the use of MoPub's services in violation of the Children's Online Privacy Protection Act (COPPA) and MoPub takes a number of steps to comply with these obligations.

MoPub Publisher Partners—companies that develop mobile applications (or "apps" as they are more commonly known) and integrate the MoPub Services to show in-app advertising—are explicitly required to comply with COPPA in the collection and use of "Personal Information" from children under 13 years old.

Since April 2014, MoPub's Publisher Policy has prohibited Publisher Partners from registering for MoPub's Services if any of their apps are either (1) directed to children under age 13 (even if children are not the app's primary audience), or (2) collect information from children that Publisher Partners know are under age 13. Violations of MoPub's Publisher Policy and Terms of Service will subject a Publisher Partner's account to immediate termination.

In certain limited circumstances, MoPub permits Publisher Partners operating child-directed apps to use the MoPub Services under separate agreements with robust requirements related to COPPA compliance. These agreements require Publisher Partners to designate their apps as "child-directed" or "mixed audience," as appropriate, in MoPub's systems. If marked as "child-directed," all traffic from such app to MoPub will be flagged by MoPub as "COPPA traffic." If marked as "mixed audience," the Publisher Partner is required to implement age-gating. Where a Publisher Partner identifies a user as under age 13, MoPub will flag traffic from that user as "COPPA traffic." The flags identifying traffic as "COPPA traffic" allow MoPub and its Partners to identify and exclude children under age 13 from personalized advertising, in full compliance with MoPub's policies.

MoPub reviews apps that are categorized by a third party vendor as potentially appealing to children. If MoPub determines, based on an independent review, that such flagged apps are child-directed (and is not from a publisher who has agreed to our separate COPPA compliance requirements), we take immediate action to remove such apps from the MoPub platform.

MoPub's Privacy Policy expressly bars all MoPub Partners from using MoPub's Services to collect personal information from apps directed to children under the age of 13 for purposes of personalized advertising. Consistent with COPPA's exception for "internal operations," however, MoPub's Advertising Demand Policies allow MoPub partners to use this information solely for "frequency capping and contextual advertising (the delivery of advertisements based upon a consumer's current visit to a web page or a single search query, without the collection and retention of data about the consumer's online activities over time)." Since July 2013, MoPub's Policies for Advertising Demand Partners (companies that advertisers work with to bid on ad inventory through the MoPub advertising exchange and to serve ads most relevant to app users) also prohibit partners from serving interest-based advertising to inventory flagged as "COPPA traffic."

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO DAMIEN KIERAN

Question 1. Positive Aspects of State Laws/GDPR: Your company has called for a national privacy framework in order to avoid a patchwork of state laws which you have to comply with as your data travels across state lines. From an international perspective, Europe has GDPR. You have operations around the country, and some around the globe and have seen firsthand how these laws are being implemented.

Are there any states that you believe have the right framework, or aspects, in place?

Twitter believes the time is right for industry, civil society, and government to work together to develop a robust privacy framework that protects individuals' rights by ensuring transparency and accountability while preserving the freedom to innovate. Any robust privacy framework should: aim to increase transparency for consumers so that they understand what data is collected about them, what that data is used for, and when it is shared; grant users meaningful control over what data is collected about them, how it is used, and when it is shared; stipulate that consumers should be able to see and change information companies have about them; requires thoughtful data collection so that only the data necessary to provide the best possible services for consumers is collected; and ensure that companies are accountable to consumers including by conducting rigorous reviews of how personal data is collected and used and that organizational mechanisms are in place to identify and vindicate consumer's right to privacy.

Question 2. Can you point to an aspect of the California law that you believe is reasonable and should be emulated on the national level?

Answer. We believe that the underlying goals of the California law should be emulated in a national level legislation.

Question 3. Nevada passed a privacy notice law during the 2017 session, how is your company doing in complying with this?

Answer. Nevada's 2017 privacy notice law is consistent with transparency steps that Twitter has long taken seriously. By requiring companies to disclose the categories of information they collect through its website or online services, and any third parties with whom that information may be shared, a description of review and change the information collected, a description of the process used to notify people of material changes to the notice, users of material changes to the notice, a disclosure of whether third parties may collect information about users' online activities from the service, and the effective date of the notice, the notice law drives companies to be accountable to the people that use their services.

Question 4. What part(s) of the GDPR should we look to emulate in the U.S.?

Answer. Twitter believes that both the California Consumer Privacy Act and the GDPR provide good foundations when considering Federal legislation. The GDPR was crafted over a number of years, and while it is EU-centric and sensitive to EU concerns, the objectives of the GDPR—to ensure the protection of privacy as a fundamental right—is borne out in the carefully considered language it contains. That said, there are areas where Twitter believes adjustments should be made to the GDPR as its concepts are considered by lawmakers contemplating potential Federal legislation in the United States. This includes specific language around automated decision making. In addition, although Twitter believes that people should be able to erase the information they provide to a service—and Twitter provides people the ability to erase their data—we believe that the commonly titled "right to be forgotten" in the GDPR is inconsistent with concepts and traditions around free speech, journalism, and "right to know" consumer benefits.

Question 5. State Attorneys General: I understand the utility of having a national framework given how difficult it would be to develop 50 different frameworks based on state law. At the same time, we want to ensure that states play a role in protecting the privacy of their residents.

What should, in your view, be the role of State AGs in enforcing privacy standards?

Answer. Twitter believes that, generally speaking, state attorneys general have an important role to play in enforcing privacy standards. We believe that as part of a comprehensive Federal legislation there is room to ensure that specific enforcement mechanisms exist to ensure that the rights of individuals are protected.

Question 6. Law Enforcement: I believe our law enforcement officials should have a mechanism to obtain the data they need for legitimate investigations. At the same time we need to strike the right balance between keeping our country and communities safe while protecting individuals' civil rights and privacy. Your company has access to many of the personal and intimate choices of millions of your customers, data and records that paint the picture of the everyday lives of millions of American families.

How do you believe a national privacy framework could seek to strike the right balance?

Answer. Twitter has positive relationships and works collaboratively with law enforcement around the country. To protect the people that trust us with their data, however, requires valid legal process before law enforcement may obtain information from Twitter. Any national framework should balance the interests involved to ensure that law enforcement entities may continue to obtain the information they need when valid legal process has been obtained, while also ensuring that people's data is protected from inappropriate or unreasonable searches and seizures.

Twitter responds to valid legal process issued in compliance with applicable law. We provide clear guidelines for law enforcement at *https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support.*

Twitter's policy is to notify users of requests for their Twitter or Periscope account information, which includes a copy of the request, as soon as we are able (*e.g.,* prior to or after disclosure of account information) unless we are prohibited from doing so by law (*e.g.,* by an order under 18 U.S.C. § 2705(b)). We ask that any non-disclosure provisions include a specified, limited duration (*e.g.,* 90 days) during which Twitter is prohibited from notifying the user. Exceptions to user notice may include exigent or counterproductive circumstances, such as emergencies regarding imminent threat to life, child sexual exploitation, or terrorism.

Question 7. Privacy Enhancing Technology: There are many technologies that actually enhance users' privacy: Encryption, anti-virus, cybersecurity technologies are all examples of this. I think this is a portion of the privacy debate that sometimes gets looked over, but one we should consider as we look at privacy legislation.

Can you summarize some of the privacy enhancing technology used at your company?

Answer. Privacy is part of Twitter's DNA. Privacy has been part of Twitter's DNA since it was created almost thirteen years ago. When Twitter was founded it was decided that people should be able to create accounts under a pseudonym. That deliberate design, combined with the granular privacy controls we provide, has enhanced privacy protections for people who use Twitter around the world. We are constantly looking for ways to evolve and employ technology to ensure the privacy and security of the data of our users. This includes, for example, our information security team constantly assessing tools that we could implement to detect and prevent internal and external data protection threats.

Question 8. Do you believe the Federal Government could assist in either funding the development of similar technologies or establishing a framework for companies to implement them into their data processing?

Answer. Twitter believes that the Federal Government has an important role to play in encouraging the continued development and innovation of privacy protections by creating and supporting environments where new initiatives could be tested.

Question 9. Small Business: As we talk about a national framework, one of the most important things to keep in mind is how we work with small business. Your company has the ability to maintain cybersecurity and compliance teams that make it easier for your companies to work with any potential law we pass.

Can you discuss how your companies might be working with, or aiding, small businesses with their privacy and data needs?

Answer. At Twitter, we are focused on providing the best possible service for our users while protecting their privacy and complying with all relevant data protection laws.

Question 10. Also, can you provide your thoughts on how a Federal framework would best take the challenges and opportunities of small businesses into account?

Answer. Twitter employs approximately 3,800 individuals globally. As a modestly-sized company in comparison to some of our peers, Twitter urges Congress to consider the resources and costs associated with complying with increased regulation. One way to avoid costly compliance costs is to set nationwide privacy standards that would harmonize that regulatory landscape and prevent a patchwork of state laws.

Question 11. Data Protection Officers: As you all 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 company's perspective on this requirement?

Answer. Twitter believes that the Data Protection Officer plays a critical role in identifying and implementing best privacy practices. The duties of a Data Protection Officer include: working towards the compliance with all relevant data protection laws, monitoring specific processes, such as data protection impact assessments, increasing employee awareness for data protection and training them accordingly, as well as collaborating with the supervisory authorities. We believe that appropriately appointed and provisioned Data Protection Officers present a key component in providing real and effective accountability within companies with respect to data protection.

Question 12. Data Minimization: One component of the GDPR is a concept known as "data minimization." This principle states that data processing should only use as much data as is required to successfully accomplish a given task and data collected for one purpose cannot be repurposed without further consent. The idea behind this is both to ensure that users are comfortable that their data is only being used for the purposes which enhance the experience and also help limit the impact of any data breaches.

It seems like there may be challenges to implementing something this broad, especially as it is laid out in the GDPR, but it nonetheless feels like something that should be explored as part of our conversation here in the United States.

What is your company's perspective on this requirement?

Answer. Twitter believes that privacy-by-design is key to accountable data protection practices and we are already working to ensure these concepts are embedded in they way our teams work at Twitter. Twitter believes that we should only collect and use personal data to provide the best possible services that our users deserve and expect this includes ensuring that we have appropriate retention periods for personal data.

Question 13. 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.

Do you build your own data centers or contract with another entity?

Answer. Twitter does not own its own data centers and contracts with other entities for such services. To the extent Twitter transfers, stores, or otherwise utilizes personal data we work to ensure security over such data management and we work with industry partners to do the same, consistent with contractual obligations and applicable laws.

Question 14. What steps do you take to secure these centers?

Answer. Please see above.

Question 15. How often to you review your physical data security standards at your data centers?

Answer. Please see above.

Question 16. Data Use: Under Twitter's privacy policy, Twitter will "store and process your communications and information related to them." What does this entail?

Answer. In order to provide our Direct Messaging services we must be able to receive, transfer, and store the information within the messages. We do this in compliance with the entirety of our Privacy Policy. Other than to ensure Direct Messages

do not contain spam and to ensure the safety and security of the platform, we do not use the contents of Direct Messages.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO GUY "BUD" TRIBBLE

Question 1. Efforts to draft meaningful Federal legislation on consumer data privacy will heavily rely upon determinations of what types of personally identifiable data are classified as "sensitive" and what are not. While some have suggested that expanded FTC rulemaking authority is necessary to flexibly account for new types of data sets coming from innovative technologies, I have concerns that excessive rulemaking authority could lead to frequent reclassifications of the types of data with ensuing liability adjustments. Do you have suggestions on how to best identify "sensitive" personally identifiable information?

Answer. At Apple, we appreciate that information cannot be handled in a one-size-fits-all manner. The appropriate treatment of personal information depends on many factors, including the nature of the personal information (such as how sensitive the personal information is), the volume of personal information, the use to which the personal information will be put, and more.

That being said, companies and innovation thrive in stable environments, where new ideas can be explored within known frameworks. And, although technological developments have changed how people see and interact with the world around them, the categories of information that people hold close has been relatively stable over time. For example, people treat their financial information with great care, maintain the confidentiality of their government identifiers such as Social Security numbers, and believe their medical and health information should be private. Legislators can look to these long-held norms and expectations of consumers to enumerate a set of data categories identified as sensitive personal information in Federal privacy legislation.

Question 2. NTIA issued a request for comment on ways to advance consumer privacy without harming prosperity and innovation. I commend the administration for their attention to this important issue. The "High Level Goals for Federal Action" that NTIA is seeking comments for includes inter-operability and the development of a regulatory landscape that is consistent with the international norms and frameworks in which the U.S. participates. How do you foresee Federal legislation affecting cross-border data flows?

Answer. In today's interconnected world, any legislation or technological change that affects information necessarily has ripple effects throughout the global digital economy. As a leader in technology and innovation, the United States is well-positioned to impact not only how data is handled within its borders, but around the world. The U.S. should seize this opportunity to create strong Federal privacy legislation that sets a minimum floor for the responsible handling of personal information by companies doing business within its borders, or otherwise handling the personal information of individuals in the US. The legislation should include bolstered FTC authority with materially significant sanctions for the violation thereof. Because a person's interest in protecting their data does not stop at the national boundary, nor should the obligations to maintain reasonable privacy and data security standards to safeguard personal information. We would urge the Committee to consider developing and applying minimum standards to protect the privacy and security of personal information of individuals in the U.S. regardless of the company's location or where the data is stored.

Question 3. Also included in NTIA's request for comments, how should the U.S. government encourage more research and development of products and services that improve privacy protection?

Answer. At Apple, we believe that great products do not need to come at the expense of user privacy. Responsible innovation means carrying out research and development with privacy in mind. That is why we focus on techniques like on-device processing to avoid the need to collect user data, differential privacy to provide greater anonymity for users when we collect data, and intelligent tracking prevention. Legislation also plays an important role in incentivizing behavior and shifting norms. Well-crafted Federal privacy legislation could help to encourage the research and development of products and services that improve privacy protections by requiring that companies put consumers in control of what personal information is collected and how it is used and shared. Legislation could also look to address the technical aspects of how companies process personal information that they have collected and encourage the use of privacy-protective techniques like anonymizing or de-identifying data. For example, we associate Apple Maps data with temporary

random identifiers, not a user's Apple ID, meaning Apple can provide users with relevant information without building a history of their location.

We believe that comprehensive privacy legislation should also include accountability mechanisms, requiring that companies develop and maintain privacy and data security programs to protect the information entrusted to them by consumers. Such legislation should also allow for flexibility in such programs to encourage companies to create programs tailored to the nature and volume of personal data processed, and the risks posed by the company's activities. Depending on the legislation, it may be appropriate to introduce a safe harbor for companies that have appropriately implemented specified safeguards or employed other specified privacy techniques, such as certain encryption standards, to protect the personal information of consumers. Finally, the legislation should include strong sanctions to deter the violation thereof.

Question 4. 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. Apple believes that a user's data belongs to them. And Apple believes that consumers should be in control of the information that they provide about themselves. We support the GDPR's efforts to promote consumer control in the right to portability and the right to be forgotten as well as other mechanisms to make sure consumers are in control, such as the right to opt out of the use of their personal information, or the ability to correct their personal information.

We appreciate this Committee's identification of the practical challenges associated with implementing requests by consumers to exercise their rights under GDPR. It is important that tools designed to empower consumers are designed thoughtfully so as to avoid unintended consequences and impractical results. For example, these rights should not require companies to delete data maintained about known fraudsters. And, once personal information about a consumer has been incorporated into the output of a proprietary algorithm, a company should not be required to destroy company property—in the form of a proprietary algorithm—to satisfy a consumer's request to delete their information. Instead, the rights granted to consumers and the technology industry's corresponding obligations should take into account technical feasibility, the encouragement of innovation, the welfare of consumers, and the interests of the general public, in their development and execution. By considering a well rounded set of factors in developing consumer rights and business obligations, we believe that legislators could achieve the aim of putting consumers in control of their own information without unnecessarily or unintentionally harming innovation.

Question 5. 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. Apple believes that any information that relates to an identified or identifiable individual is personal information; and that no privacy legislation should require companies to re-identify or otherwise increase the identifiability of information they maintain. If the results of an algorithm relate to an identified or identifiable individual, then those results are personal information. Whether the results must be deleted or transported at the request of the consumer depends on the nature of the results and of the consumer. Is there a lawful reason for why the personal information should not be transported? For example, are the results from a proprietary security or fraud prevention algorithm, the disclosure of which would assist a bad actor in committing further fraudulent acts? At Apple, so long as the information relates to an identified or identifiable individual, any applicable consumer rights apply unless there is a countervailing lawful interest that applies; and the GDPR fully recognizes and is aligned with these concepts.

Question 6. Since companies often use aggregated data outputs to study and improve their existing algorithms, services, and products, what impacts do you expect these vague GDPR requirements to have on companies' abilities to innovate?

Answer. We believe companies should challenge themselves to reduce the identifiability of information that they hold, and aggregating data is one way of doing so. We believe that meaningful privacy legislation should encourage companies to take these steps, and shouldn't require companies to re-identify data that is not held in an identifiable way. Encouraging responsible behavior, including reducing the amount of identifiable data collected and retained by companies for unnecessary or

unlawful purposes, is a vital part of protecting user privacy while retaining pathways for innovation. We believe it is too early to tell how the GDPR's provisions will generally impact the technology sector's ability to innovate or the methods used, but would encourage this Committee to take the impacts into account as it undertakes the task of crafting Federal privacy legislation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELLEY MOORE CAPITO TO GUY "BUD" TRIBBLE

Question 1. According to a study by Pew Research, only 38 percent of consumers know how to limit what information they give online. Consider me among those consumers who do not know what is being collected and how to keep my information to myself. Even with privacy settings and assurances that my data is not being collected and used without my consent, I still have concerns.

I believe the root of this issue is transparency and consumer confidence. What are your companies doing to increase the transparency when it comes to the type of data you collect?

Answer. Apple believes that consumers own their personal information and therefore must be in control of their own information. The first step in putting the consumer in control is developing tools to help ensure that the consumer has all relevant information about how their personal information is being handled, at the time they need that information.

Apple has dedicated teams focused on how best to provide consumers with the information and tools they need to take control of their personal information. Throughout its history, Apple has developed and implemented a suite of innovative and privacy-protective tools. For example, we developed a privacy icon, which appears when a consumer launches or signs into an Apple service or feature that collects personal data, to make it as easy as possible for consumers to recognize when their data is being collected by Apple. We also provide users with meaningful information about their privacy choices immediately next to the mechanism they can use to exercise that choice, to make it as easy as possible for consumers to make informed decisions about their privacy.

Apple doesn't just hold itself to high standards, it also encourages App Developers to engage in the responsible collection and use of personal information through its app developer Program License Agreement (PLA) and our App Store Review Guidelines which have extensive privacy requirements. Apple also helps to ensure that the app developers comply with the terms of the PLA by creating technical controls to enforce requirements. For example, Apple provides technical controls via the operating systems we develop to require that an app developer that would like to access location information must explicitly ask and provide the consumer with an explanation as to why it would like to access the location information, before iPhone will allow access. These are just some of the ways that Apple works to help ensure that consumers are given the information they need to exercise informed choices about their information. And, because privacy is a core value at Apple, our job in protecting consumer privacy is never done—we are continuously challenging ourselves to improve our privacy protections and keep consumers in control of their data.

Question 2. What difficulties have your companies faced when developing more transparent privacy policies?

Answer. Apple is deeply committed to the concepts of transparency, consent, and control so that users have the information and the tools available to make informed privacy choices. We believe in telling our users up front exactly what's going to happen to their personal information, and asking for their permission before they share it with us. And if users change their mind later, we make it easy to stop sharing with us. Every Apple product is designed around those principles.

When Apple does ask for permission to use personal information, it's to provide our users with a better experience.

Apple's privacy policy is one of many places that users can go to learn about how Apple handles their personal information and how they can exercise their rights in their data. Apple has worked to help ensure that its privacy policy is useful to consumers, by using clear and plain language, altering font size to draw attention to key issues, and by layering the policy so that consumers can learn even more about practices that they are interested in by clicking on links to additional information.

Recently we introduced a new privacy icon to give our customers just in time privacy notices:

The icon is shown when a user launches or signs into a service or feature that collects personal data. Underneath the icon is an explanation of the key privacy practices for that product or service followed by "See how your data is managed" link with more fulsome details. Importantly, the icon is not shown when a user launches a privacy by default service such as Siri or Maps which doesn't collect personal data.

As the digital economy becomes increasingly complex, it is likely that consumers will be presented with even more information about how their data will be collected and used. One of the key challenges facing industry and legislators today is how to ensure that consumers are provided with the information they need at the time that they need it—in other words, by focusing on not just transparency, but pertinence. We believe that a privacy policy is a useful tool—but not the only tool—that companies should offer consumers to help them learn more about how their data is handled. At Apple, we work to meet that challenge by providing consumers with privacy policies, just-in-time notices, and meaningful controls. As this Committee takes up the difficult task of Federal privacy legislation, we would encourage it to challenge companies to come up with creative ways to provide consumers with relevant information about their privacy practices at the time that consumers need that information to make a decision, to help consumers them stay in meaningful control of their personal information.

Question 3. West Virginia has a high elderly population that is rapidly increasing as baby boomers retire. I am positive that a lot of my elderly constituents are among those individuals who do not know how to limit their online information.

What are some of the measures your companies are doing to teach consumers—and specifically older consumers—about what data they share on your platforms?

Answer. As a company dedicated to creating great products for peopleof all ages and backgrounds, we understand that people experience technology differently. That is why we provide information about our products and services—including our privacy practices—in a variety of ways, to help ensure that, no matter what consumers are looking for, there is a solution that works for them.

On our website, at www.apple.com/privacy, consumers can learn more about how our products work. Apple's privacy policy provides an overview of Apple's approach to privacy and how we handle personal information. And we provide just-in-time privacy notices with detailed information about Apple's handling of personal information, together with our Apple privacy icon, to help alert users to particular privacy practices when they become relevant. Interested consumers can review detailed information on the technical safeguards we have built in our iOS Security Guide and macOS Security Overview.

Consumers can also contact Apple by phone, e-mail, or text, or visit us in a retail store to learn more about the tools that they can use to control their personal information and to have trained personnel help walk them through how to take certain actions, such as how to enable location Services or change other settings.

Question 4. I know advertising through data collection has a monetary value, and appreciate the business model, however, I find it hard to know what is being collected and how I can keep my information to myself. Even with privacy settings and assurances my data is not being used without my consent, I still have concerns.

Please explain how your business model allows both data to be used to make suggested recommended purchases on your site? As well as how you use that data to target ads to consumers? And how do you do that while protecting personal data?

Answer. Apple's online store does not create user profiles based on personal information collected from third parties to recommend purchases. We do use the information you expect us to know about your Apple online store activity to personalize your experience; for example, if you purchase an iPad, you may be shown an iPad case or cover. To help consumers navigate the thousands of apps made available on the Apple App Store, we offer the ability to personalize the App Store experience. Consumers can turn off App Store personalization at any time by disabling the "Personalized Recommendations" switch. When personalization is enabled, we use information about a consumer's use of the App Store, such as the content searched for, downloaded and purchased, to suggest relevant apps. We accompany this with a transparency page which makes clear to the user what data was used to personalize their Store experience.

Apple also helps its developers promote their apps by advertising on the App Store. Even so, because privacy is a fundamental value at Apple, we have taken additional steps to help ensure that consumers' identity and other personal information remains protected: Apple does not allow developers to target specific individuals or even groups of a handful of individuals. Instead, consumers are grouped in buckets of at least 5,000 consumers to help ensure that no one consumer's identity or

characteristics is known or knowable. Finally, consumers can opt out of targeted advertising by Apple entirely, at any time, by enabling "limit Ad Tracking."

Question 5. How can Congress ensure that data collected is used responsibly without shutting down the collection of data completely?

Answer. The digital economy runs on information. For the economy to continue to succeed, it must be built on a solid foundation of trust between consumers and companies, grounded in a common understanding of how information will be collected and used. In enacting comprehensive Federal privacy legislation, Congress can help establish that common understanding by setting minimum standards for the collection and treatment of personal information by companies operating in or otherwise handling the personal information of individuals in the US. Doing so will help set the groundwork on which a vibrant digital economy can flourish.

To help ensure that technological innovation can and does continue, any legislation should acknowledge and leave room for responsible innovation—including with respect to privacy—protective technologies. In all industries, but particularly in the digital economy, the technology of tomorrow is light years beyond the technology of today. Therefore, to help enable privacy innovations and help ensure the protection of the personal information of consumers, we encourage this Committee to consider establishing a framework for data protection that ensures consumers have robust and enforceable protections and incentivizes companies to innovate, develop, and deploy new and meaningful privacy-enhancing technologies.

Question 6. In April, the European Union (EU) passed the General Data Protection Regulation (GDPR) in order to protect personal data and uphold individual privacy rights. These new regulations have created uncertainty for U.S. firms, despite several already coming into compliance.

Innovation is important to small businesses, especially in rural America. The new European standards have created massive hurdles for these businesses to be in compliance. Many small companies in Europe are already expressing an inability to afford the legal consequences. For example, if a rural grocery store advertises online and provides a link to coupons. Under the GDPR compliance rules, this simple practice can result in extensive legal consequences.

For those who do business in Europe, do you think GDPR has the potential to have negative impacts on rural small businesses in Europe?

Answer. As the GDPR has only recently come into force, it is too soon to assess the administrative impact of the legislation on businesses and how potential penalties may affect the market. GDPR acknowledges that special considerations in relation to record-keepingmay be present for small-and medium-sized enterprises (generally understood to be companies with under 250 employees). More generally, some GDPR requirements may serve to help smaller businesses by spurring competition, such as the right to data portability. In large part, the impact of GDPR on small businesses will be left to the discretion of the enforcement bodies, the data protection authorities.

We believe that well-crafted comprehensive privacy legislation should impose obligations on businesses that are appropriate given the potential risks to consumers and the public. We appreciate the challenge that this poses and would encourage the Committee to look to the provisions and impact of all existing privacy and data security legislation as it looks to craft a Federal law.

Question 7. California has already passed a sweeping consumer protection law that threatens established business models throughout the digital sector. I appreciate the industry taking the initiative in creating a framework, in addition to the privacy principles released by the U.S. Chamber of Commerce.

As we begin discussing the appropriate position of the Federal government, can you describe what actions we should investigate more closely for any potential national framework?

Answer. The United States has taken a reasoned and measured approach to legislating the flow of information, which provides it with benefit of learning from the successes and challenges of various data protection regimes around the world, as well as sectoral laws in the United States. We would encourage this Committee to take into account all available information regarding the language and effect of laws governing the handling of personal information as it considers comprehensive Federal privacy legislation.

In the United States, for example, the Federal Privacy Act of 1974, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act all serve as useful data points to consider regarding the appropriate governance of personal information. States have also served their role as laboratories in enacting similar but differing laws in areas such as data breach notification and financial privacy. Globally, the European Union's GDPR and

the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System should provide further source material.

In addition to existing legislation, we also believe that consumer concerns and the characteristics and limitations of technologies (as well as the need for flexibility to accommodate future technologies) should be taken into account. Importantly, to help ensure that legislation does not unnecessarily stifle innovation and economic development, we would encourage this Committee to consider the impact on consumers, businesses, and the public and find the appropriate balance when considering legislation.

Question 8. Who, in your opinion, is the appropriate regulator to oversee any framework and why?

Answer. Any regulator tasked with overseeing Federal privacy legislation should be armed with resources and knowledge, including technical experts, to appropriately enforce meaningful Federal privacy legislation. As the current leading Federal privacy enforcement agency is the Federal Trade Commission, we believe the FTC should play an important role in interpreting and enforcing comprehensive privacy legislation.

Question 9. According to recent research by Magid, a media research firm, 35 percent of millennials share their password to access streaming services. I certainly understand that the terms and conditions of these services already note that access is for personal use and not to be shared with others. And that the account holder remains responsible for the actions of that third party. However, as the number [of those in the] younger generations sharing their password grows so has the potential for abuse. This "overly sharing of passwords" and the younger generation operate differently than many my age.

Are your policies flexible to cover a third party that may use a friend's or spouse's password? Is this something we should consider as we create Federal guidelines?

Answer. Meaningful privacy controls are built upon great security and need security to function properly. Whenever data security controls are compromised, the safety and confidentiality of data is put at risk. This is true even where passwords are shared with friends or loved ones, as such sharing creates another avenue through which a bad actor could attempt to gain access to a consumer's account.

As part of Apple's commitment to privacy, we challenge ourselves not to take steps that would decrease the security of consumers' information—we believe there is a better way. When Apple was confronted with the problem of sharing of passwords among family and friends, instead of encouraging such security-weakening behavior, Apple worked to develop a means for consumers to share information and activity with their friends and loved ones through Family Accounts, which allow users to share media they have purchased, including movies, songs, apps, and books, among accounts that share one payment method. We challenge ourselves to incentivize everyone in the ecosystem to allow for great experiences while leaving passwords—and personal data—under the control of individual people.

Response to Written Questions Submitted by Hon. Todd Young to Guy "Bud" Tribble

Question 1. GDPR establishes a right of data portability, which some believe is key to driving new innovation and competition within the emerging data ecosystem. Others are concerned that data portability rights, depending on how crafted, could further entrench incumbent companies.

What questions should policymakers be asking in developing data portability rights?

Answer. Data portability and data access are used somewhat inter-changeably. Data access is the right to access all personal information stored about you, with very limited exceptions by a company or organization. It is a cornerstone of privacy as it allows for an individual to know what an organization holds on them and then act appropriately. Data portability is a new concept introduced by the GDPR that could also help drive innovation and competition in the global digital economy. As with other rights, such as the right to deletion, it is important that the right is properly scoped, so that bad actors cannot perversely use the rights to harm others. For example, a person should not be able to port all information that a company has about them, regardless of source. Doing so would sweep up information provided about them to the business by other persons, to which they would otherwise have no right. Doing so would also sweep up internal proprietary information about a company's fraud and security efforts that, if ported, could divulge trade secrets and/or confidential security information to potential bad actors. It is a right that is very much in its nascent stage and while we have enthusiastically sought to give effect

to it under GDPR, it does need more time to fully develop. We would encourage the Committee to adopt a data portability mandate, bounded by firm guardrails, to help ensure that this right serves to further empower consumers and not create new or unforeseen consumer risks.

Question 2. What improvements would you make, if any, to Art, 20 of GDPR, which addresses the right to data portability?

Answer. As you know, Art. 20 of the GDPR requires that companies maintain the information to be ported in a standard format or to have the ability to move the data into that format. As technology continues to evolve, moving data to a standard format may not be feasible, especially given the speed at which innovation occurs. And, doing so may be cost-prohibitive for small businesses who lack the resources to move data into a "standard" format.

Question 3. How best can data portability rights be crafted to create new competition, but not further entrench incumbent companies?

Answer. As the GDPR is still young, it is difficult to tell what aspects of the right to data portability will operate as intended to create new competition and what might result in the entrenchment of incumbent companies. We look forward to learning more as enforcement begins and matures. However, we do believe that, in order to help ensure that competition is created, new entrants and small businesses should not be driven out of business as a result of the requirement itself. For example, a new entrant or small business should not be required to transfer personal information to a "standard" format if doing so would be cost-prohibitive. We look forward to continuing to work with the Committee on this and other issue as it considers comprehensive Federal privacy legislation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO GUY "BUD" TRIBBLE

Question 1. When devices get old they get to a point where they cannot support updates for the device operating system or the many applications run on the device. What is the obligation of the device manufacturer's, operating system programmers, and app developers and programmers regarding to older devices?

Answer. The exciting pace of technological innovation today is unprecedented. And, the novel developments of today quickly become outdated. Eventually, today's hardware will be unable to support the engineering feats of the days to come. Software developers should also ensure that they have clearly communicated any hardware requirements or other specifications that must be met in order for the software to function as intended so that consumers can make informed decisions about what software they would like to install on the devices that they have purchased.

Question 2. What guidelines do your companies follow when it comes to communicating with consumers when either the hardware or software they are using can no longer support updates-especially when these updates relate to security? Is there an industry wide practice that applies here?

Answer. We believe it is important that companies communicate material facts about hardware or software releases to consumers so that they can make informed decisions about how to use products and services and whether to install certain software. Apple considers information about the security of its software to be important, and makes this information available on its webpage, at *https://support.apple.com/en-us/HT201222.*

As Apple software updates are available via the App Store, App Store standards apply to such communications. Other standards may apply in other contexts.

Question 3. What is a reasonable consumer expectation with regard to how long the device will be viable?

Answer. We understand that consumers may conclude a device is no longer viable if the hardware itself breaks or if the hardware components are no longer capable of supporting current versions of software. At Apple, we build our products to last and believe that, if well cared for, Apple devices could last a lifetime. We appreciate that the pace at which software technology innovation is occurring today can bring material changes to computing in a short period of time. How long it takes for software changes to stretch the capabilities of older hardware depends on the hardware, the particular change to the software, and the type of use that the hardware owner engages in—a person that uses a device for basic functions may be able to use the device for many years beyond what a heavy user or sophisticated user would consider viable.

Question 4. The EU has considered promoting a voluntary labeling system informing consumers about a product's durability, upgradeability and reparability. What do you think of this idea?

Answer. We support efforts to provide consumers with meaningful information about the goods and services that they purchase. We believe, however, that given the pace of technology, it may be impossible to determine with accuracy a product's durability, without knowing in advance tomorrow's technical improvements. But, we support efforts to provide consumers with information that they need to make informed decisions.

Question 5. Should devices come with an expiration date in order to manage consumer expectations and more importantly their awareness of their online safety?

Answer. We believe that expiration dates should be used where consuming or using a product past that expiration date will result in harm to the consumer. Providing expiration dates unnecessarily contributes to global electronic waste without providing a related consumer benefit.

Question 6. In general we have been exploring the idea of opt in frameworks to keep consumers informed about what their data is being used for. However, we know from recent history that there are some uses of data that should never be permitted—like the leveraging personal data to interfere with election processes. How could we design an opt in framework that is meaningful to consumers, doesn't desensitize them to important decisions about privacy and makes sure they consent only to lawful uses of their data?

Answer. At Apple, we believe that the user should be in control of how their information is collected and used. For that control to be exercised, consumers must be able to make meaningful and informed choices about their privacy. Affirmative, or opt-in, consent is one way that consumers can express their privacy preferences. However, use of opt-in consent in all circumstances risks desensitizing consumers to important notices about their personal information. There are also situations where it would be contrary to the public interest to require opt-in consent, such as a decision by a state to automatically enroll citizens in an emergency alert or voter registration program. We believe that providing consumers with informed choices can be accomplished by using a variety of tools, including by providing users with the option to provide affirmative consent and by empowering them with easy access to privacy controls by which they can enable or disable information flows.

We appreciate the challenge facing our lawmakers today regarding the wide variety of data uses and the potential for bad actors to exploit information. Where the public has decided that certain uses of data are so contrary to the public interest as to be unlawful, such uses should be prohibited by a comprehensive privacy law such that no entity could lawfully request consumer consent to uses that have been deemed against the general welfare of the society.

Question 7. Short of regulation, what more can you and your colleagues and competitors do to restore and maintain our and our constituents' trust that you won't continue to collect more data than consumer understand, use it in ways they never imagined, and then fail to protect the data from unauthorized use and access?

Answer. Because privacy is one of our core principles, with each project, we work to challenge ourselves to minimize the personal information that we collect, to provide meaningful privacy protections and to help ensure that consumers have real choices about how their personal information is collected and used. We believe that meaningful privacy protections require a foundation in security, and we invest significantly in the design and development of security systems in our hardware, software, and services. We do not believe that a company's work here is ever done, but believe that companies should be constantly engaged in research and development to improve privacy and security protections and help ensure that consumers are in control of their information. We've proved time and again that great experiences don't have to come at the expense of your privacy and security. Instead, they can support them.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO GUY "BUD" TRIBBLE

Question 1. State Preemption: Several public interest organizations have written the Committee in advance of the hearing expressing their deep concerns about state preemption. As the ACLU noted, it has often been the states—not the Federal Government—that have acted in a timely and important way to protect consumer interests.

Please provide to me a set of recommendations for how to improve the California Consumer Privacy Act and the GDPR.

Answer. We support both the California Consumer Privacy Act (CCPA) and the GDPR's efforts to help ensure that consumers are provided with meaningful privacy rights, including the rights to transparency, access, and control. In both cases, the true impact of the legislation is yet to be seen, as the laws have just, or have not yet, come into force. With respect to the CCPA, we believe that the definitions used in the law create the potential for confusion and complication in the privacy space, as several definitions of key terms depart from common consumer understanding of the terms and well-accepted definitions of the terms in the privacy space. We would encourage this Committee to consider anew appropriate key definitions should the CCPA remain as enacted.

As the GDPR has only recently come into force, it is too soon to assess the administrative impact of the legislation on businesses and have yet to understand how potential penalties may affect the market. GDPR acknowledges that special considerations in relation to record-keeping may be present for small-and medium-sized enterprises (generally understood to be companies with under 250 employees). More generally, some GDPR requirements may serve to help smaller businesses by spurring competition, such as the right to data portability. In our experience, the GDPR's 72-hour breach notification requirement may also be improved upon. Investigations into the nature and cause of a data breach take time and are very rarely fully understood within 72 hours. Others can be completed much quicker and could be reported well within 72 hours. In more complex cases, officially reporting information to enforcement entities within that time-frame may serve to limit important investigations and introduce the need to correct the record as additional facts are learned; incomplete information may also cause unnecessary panic, while the true nature and extent of the breach continues to be ascertained. We would encourage this Committee to consider whether and how breach reporting may best provide pertinent information when that information is ripe and relevant to consumers and regulatory authorities.

Question 2. Privacy by Design: Between the six of your companies, you have access to an overwhelming amount private information about nearly everyone in the United States. AT&T and Charter have access to the browsing history of your customers. A Princeton study found that Google collects visitor data from 70 percent of websites—including from Twitter, a competitor. It's hard to imagine what your companies don't know.

Would you commit to privacy-by-design—limiting collection of data and deleting data when it is no longer useful to your customers?

Answer. Yes. We are fully committed to this principle and have time and again demonstrated it in our products and services. We also challenge ourselves to "know" as little as possible while providing world-class services. Minimizing the collection of personal data is an important aspect of privacy-by-design at Apple.

Question 3. What specific steps do you plan to take to limit your own use of customer data? Can you provide examples where you deleted or stopped collecting data to protect privacy?

Answer. Apple's internal privacy practices require that it challenge itself to collect only that information that is relevant and necessary to the purpose at hand and to only maintain that information for so long as it is needed to fulfill its purpose. Apple applies this privacy-by-design framework to each project that it engages in across all of its products and services.

Apple works to enforce privacy-by-design principles by only collecting and maintaining that personal information that is necessary at the outset, rather than realizing that it collected more information than was necessary later and deleting that information. Apple is also constantly developing and improving tools that consumers can use to indicate in real time whether they would like their information to be collected and for what purposes. iPhone users, for example, can control whether Apple or other app developers can access categories of personal information through simple switches, such as by enabling or disabling "Location Services."

Question 4. Privacy by design is fundamental to the GDPR. What specific changes have you made to your products to come into compliance to the GDPR's privacy-by-design requirements?

Answer. Privacy by design has been a foundational concept at Apple from its early days. As Apple has historically practiced privacy-by-design, no specific changes were considered necessary to the design of existing Apple products or our design approach to come into compliance with the GDPR's privacy-by-design requirements.

Question 5. FTC Rulemaking: In most of your remarks, you discuss the challenges of regulating evolving technologies and economies. It would seem to me that this requires a Federal agency that is responsive to technology changes.

Would you support the FTC having rulemaking authority to provide clarity, to address potential harms, and to ensure rules match technology changes? What sorts of areas should this cover?

Answer. Any regulator tasked with overseeing Federal privacy legislation should be armed with resources and knowledge, including technical experts, to appropriately enforce meaningful Federal privacy legislation. As a regulator with a long-established track record in privacy and security, and longestablished leadership on the issue on the national and international stage, we believe the Federal Trade Commission should play an important role in interpreting and enforcing any comprehensive privacy legislation.

Question 6. Advertising and Tracking: With ad blocking penetration approaching 20–30 percent, consumers are clearly concerned with how their data is used for advertising and tracking.

Will Apple Safari's new ITP 2.0 block tracking tags of Google and Facebook?

Answer. ITP uses machine learning to classify whether a domain has the ability to track individuals across sites, for instance through content like social widgets which are embedded into the site the user is visiting. For domains classified as trackers, ITP 2.0 will not persist cookies they try to store when embedded on other sites the user browses. If a user interacts with the embedded content and the content tries to access its own cookies, the user is then asked to choose as to whether they consent to that widget receiving data that could track them. We have published technical details on this technology at *https://webkit.org/blog/8311/intelligent-trackingprevention-2-0/*.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO GUY "BUD" TRIBBLE

Question 1. Unsurprisingly, none of your testimony speaks about potential increased penalties for a new privacy framework. The current penalty regime seems not to change corporate behavior—as we repeatedly have seen. In your opinion, are civil penalties an effective mechanism to push companies to follow the law? If not, what mechanisms would be effective?

Answer. We believe that comprehensive Federal privacy legislation should include accountability mechanisms to help encourage companies to protect the personal information of consumers and hold them accountable when they fail to do so. We believe meaningful civil penalties are an important accountability mechanism the Committee should look to when considering how best to incentivize responsible handling of the personal information of consumers. But civil penalties are not the only effective accountability mechanism, especially because enforcement processes are necessarily time-consuming, and may only be levied well after infringing conduct takes place. That's why we believe reporting and transparency obligations are important elements of encouraging accountability, and we encourage the Committee to consider a variety of means to incentivize responsible corporate behavior when crafting Federal privacy legislation.

Question 2. Mr. Tribble, in your testimony you stated that Apple believes privacy is a "fundamental human right." But do you believe that consumers must trade information about their online activity in order to have access to free websites and apps? What about access to affordable devices?

Answer. Apple believes that a user's data belongs to them and that they should be in charge of their information. This means that companies must challenge themselves to provide services in ways that do not require them to know everything about a consumer's online activity. When companies do need to know information, like a consumer's online activity, consumers should be provided with the information they need to make informed decisions about how their personal information is collected, used, and shared. Consumers may choose to make informed decisions to disclose certain personal information to support and in exchange for free—or even, paid—services. At Apple, we've proved time and again that great experiences don't have to come at the expense of your privacy and security.

Question 3. Since both Apple and Amazon's inception, 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 with Alexa and Siri. As both Apple and Amazon were creating this next generation of interfaces, what specific measures did each of your companies take to ensure that these new technologies complied with COPPA?

Answer. Apple employs privacy-by-design in all of its projects, and compliance with applicable privacy laws, including COPPA, as well as respect for consumer expectations, are top of mind throughout the design process.

Protecting the data of children is an important priority for everyone at Apple We believe in transparency and giving parents the information they need to determine what is best for their child. We work hard to offer controls for parents that are intuitive and customizable. In this respect, a child under 13 cannot create an Apple ID without their parent or guardian creating it for them through our Family Sharing process. Family sharing enables the parent/guardian to limit their child's access to certain types of content or resources through parental controls such as Restrictions, Screen Time, and Ask to Buy. See See: *https://www.apple.com/legal/privacy/enww/parent-disclosure/* for additional information.

In fact, Siri is yet another example of a service that reflects privacy by design. We recognized that users, especially parents or guardians of minors, would be justifiably concerned about a device recording the things that they say. Therefore, when a user enables Siri, their operating system assigns a random device identifier to their Siri use such that their use of Siri is not associated with their Apple ID. Furthermore, we try to keep all of a user's Siri information on their device where it makes the most sense and give them options to control how it's shared. For example, when Siri is used to search for a photo by location or album name, we don't have to send the photo to a server to get an answer. We also provide complete control to our users. Apple deletes data associated with a Siri identifier if a user chooses to turn Siri off.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO GUY "BUD" TRIBBLE

Question 1. Positive Aspects of State Laws/GDPR: Your company has called for a national privacy framework in order to avoid a patchwork of state laws which you have to comply with as your data travels across state lines. From an international perspective, Europe has GDPR. You have operations around the country, and some around the globe and have seen firsthand how these laws are being implemented.

Are there any states that you believe have the right framework, or aspects, in place?

Answer. We would encourage the Committee to consider the substance and impact of all enacted privacy and data security frameworks, both within the United States and elsewhere, when considering comprehensive Federal privacy legislation. Although it is too early to tell what the impact of the California Consumer Privacy Act will be on consumer privacy rights and the digital economy, we appreciate its emphasis on fundamental rights such as access, choice, and transparency, which help to put consumers in control. Globally, the European Union's GDPR and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System should provide further source material.

Question 2. Can you point to an aspect of the California law that you believe is reasonable and should be emulated on the national level?

Answer. At Apple, we believe that a foundational privacy right is the right to knowledge—the right to know what personal information is being processed and why, and to whom it is being disclosed. We appreciate the California Consumer Privacy Act's requirement that companies be transparent about the information that they collect and use relating to an identified or identifiable individual.

Question 3. Nevada passed a privacy notice law during the 2017 session, how is your company doing in complying with this?

Answer. Apple's privacy notice, and privacy program, was and remains compliant with the Nevada law, which we believe is an important step towards encouraging transparency about corporate privacy practices.

Question 4. What part(s) of the GDPR should we look to emulate in the U.S.?

Answer. Apple believes that a user's data belongs to them, and that consumers should be in control of the information that they provide about themselves. We support the GDPR's efforts to promote consumer control in the right to portability and the right to be forgotten as well as other mechanisms to make sure consumers are in control, such as the right to opt out of the use of their personal information, or the ability to correct their personal information.

We appreciate this Committee's identification of the practical challenges associated with implementing requests by consumers to exercise their rights under GDPR. It is important that tools designed to empower consumers are designed thoughtfully so as to avoid unintended consequences and impractical results. For example, these

rights should not require companies to delete data maintained about known fraudsters. And, once personal information about a consumer has been included into the output of a proprietary algorithm, a company should not be required to destroy company property—in the form of a proprietary algorithm—to satisfy a consumer's request to delete their information. Instead, the rights granted to consumers and the technology industry's corresponding obligations should take into account technical feasibility, the encouragement of innovation, the welfare of consumers, and the interests of the general public, in their development and execution. By considering a well-rounded set of factors in developing consumer rights and obligations, we believe that legislators could achieve the aim of putting consumers in control of their information without unnecessarily or unintentionally harming innovation.

Question 5. State Attorneys General: I understand the utility of having a national framework given how difficult it would be to develop 50 different frameworks based on state law. At the same time, we want to ensure that states play a role in protecting the privacy of their residents.

What should, in your view, be the role of State AGs in enforcing privacy standards?

Answer. We believe that an important part of comprehensive privacy legislation is accountability. We believe that state attorneys general could help to enforce a comprehensive Federal privacy law in coordination with a Federal regulator or where a Federal regulator has elected not to act.

Question 6. Law Enforcement: I believe our law enforcement officials should have a mechanism to obtain the data they need for legitimate investigations. At the same time we need to strike the right balance between keeping our country and communities safe while protecting individuals' civil rights and privacy. Your company has access to many of the personal and intimate choices of millions of your customers, data and records that paint the picture of the everyday lives of millions of American families.

How do you believe a national privacy framework could seek to strike the right balance?

Answer. We believe that law enforcement agencies play a critical role in keeping our society safe and we've always maintained that if we have information we will make it available when presented with valid legal process. In recognizing the ongoing digital evidence needs of law enforcement agencies, we have a team of dedicated professionals within our legal department who manage and respond to all legal requests received from law enforcement agencies globally. Our team also responds to emergency requests globally on a 24/7 basis.

We publish legal process guidelines for government and law enforcement agencies globally and we publish transparency reports twice a year detailing the types of requests we receive and how we respond. In addition, we regularly provide training to law enforcement officers on the types of data available from Apple and how to obtain it consistent with our legal process guidelines.

Soon we will begin the launch of an online portal for authenticated law enforcement officers globally to submit lawful requests for data, track requests, and obtain responsive data from Apple.

We are building a team of professionals dedicated to training law enforcement officers globally, which will significantly increase our ability to reach smaller police forces and agencies. This will include the development of an online training module for officers. This will assist Apple in training a larger number of law enforcement agencies and officers globally, and ensure that our company's information and guidance can be updated to reflect the rapidly changing data landscape.

Apple is committed to protecting the security and privacy of our users. We believe that the above developments and the work we do to assist investigations and uphold this fundamental commitment need not—and should not—be affected negatively by any national privacy framework.

Question 7. Privacy Enhancing Technology: There are many technologies that actually enhance users' privacy: Encryption, antivirus, cybersecurity technologies are all examples of this. I think this is a portion of the privacy debate that sometimes gets looked over, but one we should consider as we look at privacy legislation.

Can you summarize some of the privacy enhancing technology used at your company?

Answer. Apple believes that security is a key privacy principle and that without a foundation of great security you cannot have great privacy. Because of that, Apple has teams devoted to developing privacy-and security-enhancing technologies. For example, Apple uses on-device processing, whereby the processing of personal information about a consumer is done on the consumer's device and not on Apple's servers so that your device knows everything about you, but we do not. Apple's intel-

ligent tracking prevention feature for Safari limits how advertisers and others can track consumer browsing activity using cookies by deactivating cookies after certain periods of time.

Where Apple may need to collect data to provide a service—for example, navigation with Maps—we try to use temporary random identifiers so that the data isn't associated with an identifiable user.

Apple has also pioneered the large scale deployment of privacy-preserving techniques such as local differential privacy, which enables Apple to learn about the aggregate behavior of our users without seeing data that can be personally linked to any of our users.

Apple also enhances its privacy-protective technologies with each version of its operating systems. Some of the changes relate to core features of the Apple products and services themselves, such as where we enlarge the privacy options available in iOS and macOS.

In addition to the privacy features of Maps as outlined above and Siri as outlined in an earlier response, which do not collect personal data tied to the Apple ID of our users, our News service associates a user's reading activity within the News app with a random device-based identifier that we cannot link to their Apple ID. This is yet another example of where we were able to conclude that there was simply no good reason why Apple would need such data tied to the identity of our users.

On our website, at *www.apple.com/privacy,* consumers can learn about how our products work. Apple's privacy policy provides an overview of Apple's approach to privacy and how we handle personal information. We provide just-in-time privacy notices with detailed information about Apple's handling of personal information, together with our Apple privacy icon, to help alert users to particular privacy practices when they become relevant. Interested consumers can review detailed information on the technical safeguards we have built in our iOS Security Guide and macOS Security Overview.

Question 8. Do you believe the Federal Government could assist in either funding the development of similar technologies or establishing a framework for companies to implement them into their data processing?

Answer. We believe that responsible processing of personal information can be encouraged through a well-crafted, comprehensive Federal privacy law. We further believe that such a law could incentivize the development and implementation of new or existing privacy-protective technologies by requiring companies develop and implement comprehensive privacy programs, which include the adoption of adequate safeguards. We would also encourage the Committee to consider whether the introduction of a safe harbor would be appropriate in certain circumstances, such when data is protected by encryption. We would also encourage a flexible approach to such legislation, to help encourage further innovation in the space.

Question 9. Small Business: As we talk about a national framework, one of the most important things to keep in mind is how we work with small business. Your company has the ability to maintain cybersecurity and compliance teams that make it easier for your companies to work with any potential law we pass.

Can you discuss how your companies might be working with, or aiding, small businesses with their privacy and data needs?

Answer. At Apple, we are lucky enough to work with millions of app developers—many of whom are small-and medium-sized businesses—to populate the App Store. Apple encourages these app developers to engage in the responsible collection and use of personal information through its app developer Program License Agreement (PLA) and our App Store Review Guidelines which have extensive privacy requirements. Apple also helps to ensure that the app developers comply with the terms of the PLA by creating technical controls to enforce requirements. For example, Apple provides technical controls via the operating systems we develop to require that an app developer that would like to access location information must explicitly ask and provide the consumer with an explanation as to why it would like to access the location information, before iPhone will allow access.

Question 10. Also, can you provide your thoughts on how a Federal framework would best take the challenges and opportunities of small businesses into account?

Answer. We believe that meaningful Federal privacy legislation does not need to result in disproportionate harm to small businesses. To help ensure that small businesses continue to engage in the marketplace and enhance competition, we would encourage the Committee to carefully consider the benefit of any administrative or record-keeping provisions before introducing requirements where the overhead may outweigh the benefit to consumers; whether it might be appropriate to introduce cost considerations into the legislation, such that certain requirements only arise if practicable; and to consider whether certain requirements might apply only to com-

panies that process a certain volume of personal information, to help provide nascent companies with some breathing room as they begin to grow. By considering these, and other, possibilities, we believe that this Committee will have the tools it needs to help craft meaningful legislation without unnecessarily harming small businesses or competition.

Question 11. Data Protection Officers: As you all 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 company's perspective on this requirement?

Answer. Apple believes in accountability. We believe that it is important to have a comprehensive privacy program to protect the personal information of consumers and that there should be an individual or set of individuals responsible for developing and maintaining such a program.

Question 12. Data Minimization: One component of the GDPR is a concept known as "data minimization." This principle states that data processing should only use as much data as is required to successfully accomplish a given task and data collected for one purpose cannot be repurposed without further consent. The idea behind this is both to ensure that users are comfortable that their data is only being used for the purposes which enhance the experience and also help limit the impact of any data breaches.

It seems like there may be challenges to implementing something this broad, especially as it is laid out in the GDPR, but it nonetheless feels like something that should be explored as part of our conversation here in the United States.

What is your company's perspective on this requirement?

Answer. Apple believes that data minimization is a foundational privacy principle that companies should challenge themselves to uphold.

Question 13. 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.

Do you build your own data centers or contract with another entity?

Answer. Apple engages directly and indirectly in the development and management of its data centers. Apple places the utmost importance on the security of personal information and company information, which is why it is intimately involved in the handling of data in its data centers.

Question 14. What steps do you take to secure these centers?

Answer. Apple works to keep personal information in users' hands, on users' devices. When we do provide a service that involves our servers or data centers, Apple secures them using a combination of physical, administrative, and technical controls, including protecting the data with encryption with keys that Apple doesn't have. Basic physical controls such as locks and security cameras set the foundation. Administrative controls, such as the limiting of access to the data center locations as well as limiting access to systems and applications relevant to the data centers, serve to further safeguard the data centers. Technical controls reinforce the groundwork of physical and administrative controls by adding complex technical protections to the information maintained in the data centers.

Question 15. How often to you review your physical data security standards at your data centers?

Answer. We review the physical data security standards at Apple data centers on a periodic basis, the duration of which varies depending on the physical data center. In addition, Apple information security and audit functions spot-check compliance with policies and procedures, including physical security, throughout the year. Apple maintains current ISO 27001 and ISO 27018 certifications for iCloud.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO RACHEL WELCH

Question 1. Efforts to draft meaningful Federal legislation on consumer data privacy will heavily rely upon determinations of what types of personally identifiable data are classified as "sensitive" and what are not. While some have suggested that expanded FTC rulemaking authority is necessary to flexibly account for new types of data sets coming from innovative technologies, I have concerns that excessive rulemaking authority could lead to frequent reclassifications of the types of data with ensuing liability adjustments. Do you have suggestions on how to best identify "sensitive" personally identifiable information?

Answer. Charter has proposed a national privacy framework that requires "opt-in" consent for the collection, use, and disclosure of all personally identifiable information, rather than distinguishing between different categories of information which can be difficult for consumers. We believe that such a framework is more consistent with consumer expectations regarding protection of their personal data online.

Question 2. NTIA issued a request for comment on ways to advance consumer privacy without harming prosperity and innovation. I commend the administration for their attention to this important issue. The "High Level Goals for Federal Action" that NTIA is seeking comments for includes inter-operability and the development of a regulatory landscape that is consistent with the international norms and frameworks in which the U.S. participates. How do you foresee Federal legislation affecting cross-border data flows?

Answer. Charter strongly supports NTIA's call for a framework that protects individual privacy and fosters technological innovation, particularly its focus on a privacy framework that "reduces fragmentation nationally and increases harmonization and interoperability nationally and globally." Non-uniform rules can create consumer confusion and result in a patchwork of protection. Charter looks forward to the opportunity to participate in the development of the Administration's approach to consumer privacy.

Charter believes that a Federal framework that focuses on the five core principles of consumer control, transparency, parity, uniformity, and security will best protect consumers and produce the best outcomes for businesses that increasingly operate on a global scale.

Question 3. Also included in NTIA's request for comments, how should the U.S. government encourage more research and development of products and services that improve privacy protection?

Answer. Charter believes that the Federal government can play an important role in research and development of products and services that improve privacy protection, possibly through the establishment of voluntary consensus standards (such as the NIST cybersecurity framework) and potentially through targeted investments. The government should not mandate the use of particular technologies or products, however, and any such investments should be carefully targeted to avoid unintended consequences such as the creation of competitive disparities in the marketplace for products or services.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELLEY MOORE CAPITO TO RACHEL WELCH

Question 1. According to a study by Pew Research, only 38 percent of consumers know how to limit what information they give online. Consider me among those consumers who do not know what is being collected and how to keep my information to myself. Even with privacy settings and assurances that my data is not being collected and used without my consent, I still have concerns.

I believe the root of this issue is transparency and consumer confidence. What are your companies doing to increase the transparency when it comes to the type of data you collect?

Answer. Charter values and relies on the trust and loyalty of its more than 26 million residential and business customers. One of our key business objectives is to provide customers with a superior broadband experience that they value and use. An important aspect of ensuring that consumers continue to utilize all the services that the Internet has to offer is making sure that they are confident that they understand what personal information businesses collect about them and that their personal information online is protected. Charter strives to give our customers that confidence through a commitment to transparency. Our goal is to make our privacy

policy as transparent as possible and easy for consumers to understand. We constantly review and reevaluate our privacy policy based on feedback we receive.

Charter agrees that transparency is critical to improving consumer confidence in online services, and therefore supports the creation of a national online privacy framework, applicable to all participants in the online ecosystem, that includes transparency as a critical element. This ensures that no matter where a consumer goes online or where they live, they will receive a clear, concise, and easy to understand explanation of how the entity wants to collect, use, and maintain her data. Privacy policies should be separate from other terms and conditions of service. Adherence to these principles by all of the participants in the online ecosystem will give consumers the ability to weigh the potential benefits and harms of the collection and use of their personal data, and provide informed consent.

Question 2. What difficulties have your companies faced when developing more transparent privacy policies?

Answer. Our goal is to make our privacy policy as thorough and transparent as possible, and easy for consumers to understand. Balancing comprehensiveness and simplicity can be challenging. We therefore review our privacy policy on an ongoing basis and seek to improve it based on customer feedback. We recently completed revisions designed to improve our privacy policy's comprehensibility and accessibility.

Question 3. West Virginia has a high elderly population that is rapidly increasing as baby boomers retire. I am positive that a lot of my elderly constituents are among those individuals who do not know how to limit their online information.

What are some of the measures your companies are doing to teach consumers—and specifically older consumers—about what data they share on your platforms?

Answer. Charter regularly updates our privacy policy in order to make it easy for all of our customers to understand. Ensuring that all of our customers receive clear and helpful information about our services is a top priority. Further, as an Internet service provider, Charter does not sell or share any of our customer's personal data, to anyone, for any purpose. We expressly state this in our privacy policy and have also committed to provide customers notice and choice if we change our practices.

Question 4. I know advertising through data collection has a monetary value, and appreciate the business model, however, I find it hard to know what is being collected and how I can keep my information to myself. Even with privacy settings and assurances my data is not being used without my consent, I still have concerns.

Please explain how your business model allows both data to be used to make suggested recommended purchases on your site? As well as how you use that data to target ads to consumers? And how do you do that while protecting personal data?

Answer. As an Internet service provider, Charter does not sell or share any of our customer's personal data, to anyone, for any purpose. That means we do not share or sell our customers' web browsing histories or any of their online information for third-party marketing. We have expressly stated this in our privacy policy and also have committed to provide customers notice and choice if we change our practices.

Question 5. How can Congress ensure that data collected is used responsibly without shutting down the collection of data completely?

Answer. Charter supports the adoption of a national online privacy framework that starts with the consumer. The framework should focus on five core principles:

- Consumer control and meaningful consent, such as requiring all Internet entities to give consumers an "opt-in" choice for the collection, use, and disclosure of their data;
- Transparency, through clear, concise, meaningful, and readily available information about how consumers' information is collected, used, and disclosed;
- Parity, meaning a comprehensive and consistent approach to privacy that applies across the online ecosystem, in order to provide consumers with confidence that their personal information is protected anywhere they go online;
- Uniformity, in the form of a Federal framework rather than a patchwork approach of inconsistent privacy laws; and
- Security in the form of strong data security practices that include administrative, technical, and physical safeguards.

These principles will ensure that data are collected and used responsibly, and that consumers are informed and empowered to control the personal information that is collected about them online.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO RACHEL WELCH

Question 1. GDPR establishes a right of data portability, which some believe is key to driving new innovation and competition within the emerging data ecosystem. Others are concerned that data portability rights, depending on how crafted, could further entrench incumbent companies.

What questions should policymakers be asking in developing data portability rights?

Answer. Charter strongly believes that consumers should have control over how their data is collected and used. As a U.S.-based Internet service provider Charter is not subject to the GDPR, but we are watching the implementation of the GDPR carefully in order to determine how different aspects of the GDPR could be applied to a national framework in the United States. We recognize that both the GDPR and the California Consumer Privacy Act incorporate principles of data portability, and that the right to access, delete, and port data is an important part of the discussion in any privacy protection framework. There will be operational challenges in implementing any such rights, but Charter looks forward to participating in this discussion.

Question 2. What improvements would you make, if any, to Art. 20 of GDPR, which addresses the right to data portability?

Answer. Charter has been watching with interest to see how European Union member states implement the GDPR following its entry into force on May 25, 2018. Charter believes that further guidance and future enforcement actions in the European Union will provide valuable insight into the parameters of this right.

Question 3. How best can data portability rights be crafted to create new competition, but not further entrench incumbent companies?

Answer. Charter supports the adoption of a national online privacy framework that focuses on the five core principles of consumer control, transparency, parity, uniformity, and security. The obligation to ensure a consumer's data portability rights should apply to any entity that collects personal information, and the means of implementing portability should be carefully designed so that all providers can readily comply with it, in order to avoid conferring advantages on any particular company or group of companies. This will reduce consumer confusion and ensure that consumers are empowered to make choices regarding their personal information, without inadvertently creating competitive disparities. Charter looks forward to continuing to participate in the discussion of this issue.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO RACHEL WELCH

Question 1. In general we have been exploring the idea of opt in frameworks to keep consumers informed about what their data is being used for. However, we know from recent history that there are some uses of data that should never be permitted—like the leveraging personal data to interfere with election processes. How could we design an opt-in framework that is meaningful to consumers, doesn't desensitize them to important decisions about privacy and makes sure they consent only to lawful uses of their data?

Answer. It can be difficult for consumers to differentiate between, for example, sensitive and non-sensitive personally identifiable information. Charter has therefore proposed a national privacy framework for online data that requires opt-in consent for the collection, use, and disclosure of all personally identifiable information, rather than distinguish between different categories of information or contexts. We believe that an opt-in framework is more consistent with consumer expectations regarding protection of their personal data online. All entities across the Internet ecosystem must also ensure that consumer consent is purposeful, clear and meaningful.

Question 2. Short of regulation, what more can you and your colleagues and competitors do to restore and maintain our and our constituents' trust that you won't continue to collect more data than consumer understand, use it in ways they never imagined, and then fail to protect the data from unauthorized use and access?

Answer. An important aspect of ensuring that consumers continue to utilize all the services that the Internet has to offer is making sure that they are confident that their personal information online is protected. Charter strives to give our customers that confidence through a commitment to transparency, security and choice. We also review and reevaluate our privacy policy based on feedback we receive in order to ensure that policy is transparent and easy for consumers to understand.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO RACHEL WELCH

Question 1. State Preemption: Several public interest organizations have written the Committee in advance of the hearing expressing their deep concerns about state preemption. As the ACLU noted, it has often been the states—not the Federal Government—that have acted in a timely and important way to protect consumer interests.

Please provide to me a set of recommendations for how to improve the California Consumer Privacy Act and the GDPR.

Answer. Charter strongly believes that there should be a single national standard that protects consumers' online privacy regardless of where they live, work or travel. Whether a consumer's information is adequately protected should not differ based on which state he or she is logging in from. A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation on the internet—which is a borderless technology.

That said, there may be particular elements of the GDPR and the CCPA that could help inform a national privacy framework. While Charter is not subject to the GDPR, we are watching with interest to see how affected companies implement the GDPR's requirements and what lessons this experience may provide for the development of a U.S. privacy framework. Both the GDPR and the CCPA share core principles that Charter supports, including parity across all Internet entities, transparency, and enhanced consumer control. Charter also supports the recognition in both frameworks that there is no one-size-fits-all approach to data security.

There are also aspects of the CCPA that are inconsistent with the FTC's 2012 Privacy Framework. For example, the definition of personal information and what data are considered to be de-identified differ from the FTC Framework. These broad and inconsistent definitions could lead to unintended consequences, such as deleting information when it is necessary to address issues such as workplace sexual harassment. The CCPA may also unintentionally inhibit the ability of businesses and entities to comply with federal, state, and local laws or compromise companies' ability to implement legitimate cybersecurity and crime prevention practices.

Question 2. Privacy by Design: Between the six of your companies, you have access to an overwhelming amount private information about nearly everyone in the United States. AT&T and Charter have access to the browsing history of your customers. A Princeton study found that Google collects visitor data from 70 percent of websites—including from Twitter, a competitor. It's hard to imagine what your companies don't know.

Would you commit to privacy-by-design—limiting collection of data and deleting data when it is no longer useful to your customers?

Answer. Charter believes that the principle of privacy by design is one of a menu of principles that can help safeguard and protect consumer privacy. Charter looks forward to working with you and the Committee to discuss how to implement this concept in practice through a Federal privacy framework.

Question 3. What specific steps do you plan to take to limit your own use of customer data? Can you provide examples where you deleted or stopped collecting data to protect privacy?

Answer. Charter collects personal information from its broadband customers in order to render service. We do not sell or share any online personal data with third parties. We maintain a detailed records retention schedule under which Charter deletes customer data once it is no longer necessary to provide our services or to comply with the law.

Question 4. Privacy by design is fundamental to the GDPR. What specific changes have you made to your products to come into compliance to the GDPR's privacy-by-design requirements?

Answer. As a U.S.-based Internet Service Provider (ISP), Charter is not subject to the GDPR. However, we are watching with interest to see how affected companies implement the GDPR's requirements and what lessons this experience may provide for the development of a U.S. privacy framework.

Question 5. FTC Rulemaking: In most of your remarks, you discuss the challenges of regulating evolving technologies and economies. It would seem to me that this requires a Federal agency that is responsive to technology changes.

Would you support the FTC having rulemaking authority to provide clarity, to address potential harms, and to ensure rules match technology changes? What sorts of areas should this cover?

Answer. We believe that the Federal Trade Commission ("FTC") is the appropriate agency to oversee and enforce online privacy and data security. The FTC is

the Nation's leading agency when it comes to privacy enforcement, with a successful track record of bringing hundreds of privacy and data security cases. Moreover, the FTC's broad authority to safeguard consumers and enforce privacy protections across the entire online ecosystem will ensure the principle of "parity" that we believe is essential to an effective privacy framework. We believe that the FTC can fulfill this role through the exercise of its enforcement authority, but we are open to discussing the possibility of additional tools, including rulemaking authority.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TOM UDALL TO RACHEL WELCH

Question. Unsurprisingly, none of your testimony speaks about potential increased penalties for a new privacy framework. The current penalty regime seems not to change corporate behavior—as we repeatedly have seen. In your opinion, are civil penalties an effective mechanism to push companies to follow the law? If not, what mechanisms would be effective?

Answer. We believe that the Federal Trade Commission ("FTC") is the appropriate agency to oversee and enforce online privacy and data security. The FTC is the Nation's leading agency when it comes to privacy enforcement, with a successful track record of bringing hundreds of privacy and data security cases. Moreover, the FTC's broad authority to safeguard consumers and enforce privacy protections across the entire online ecosystem will ensure the principle of "parity" that we believe is essential to an effective privacy framework. We believe that the FTC can fulfill this role through the exercise of its enforcement authority, applying the penalties in the FTC Act. We are also open to discussing the possibility of additional tools for the FTC to address privacy issues, including civil penalties.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO RACHEL WELCH

Question 1. Positive Aspects of State Laws/GDPR: Your company has called for a national privacy framework in order to avoid a patchwork of state laws which you have to comply with as your data travels across state lines. From an international perspective, Europe has GDPR. You have operations around the country, and some around the globe and have seen firsthand how these laws are being implemented.

Are there any states that you believe have the right framework, or aspects, in place?

Answer. Charter believes that there is a need for Congress to act at the Federal level and implement a national, uniform online privacy framework. A Federal vacuum will result in a patchwork of inconsistent state laws resulting in uneven protection and greater consumer confusion.

Question 2. Can you point to an aspect of the California law that you believe is reasonable and should be emulated on the national level?

Answer. The California Consumer Privacy Act of 2018 (CCPA), which does not go into effect until January 2020, responds to the growing interest in passing legislation to protect consumers' online privacy. Charter is watching closely to see how the California law is implemented. The CCPA contains some of the core principles that Charter supports, including parity across all Internet entities, transparency, security and enhanced consumer control. There are also aspects of the CCPA that are inconsistent with FTC definitions such as the definition of personal information and what data are considered to be de-identified.

Whatever the merits of particular aspects of the California law, however, Charter believes that there must be a single national privacy framework that protects consumers' online privacy regardless of where they live, work or travel. Charter looks forward to working closely with you and the Committee to craft this framework.

Question 3. Nevada passed a privacy notice law during the 2017 session, how is your company doing in complying with this?

Answer. Charter is in compliance with Nevada's 2017 privacy notice law.

Question 4. What part(s) of the GDPR should we look to emulate in the U.S?

Answer. Charter strongly believes that consumers should have control over how their data is collected and used. As a U.S.-based Internet Service Provider (ISP) Charter is not subject to the GDPR, but we are watching its implementation carefully to see how affected companies fulfill its requirements and what lessons this experience may provide for the development of a U.S. privacy framework. The GDPR contains some of the core principles which Charter supports, including parity across all Internet entities, transparency, and enhanced consumer control.

Question 5. State Attorneys General: I understand the utility of having a national framework given how difficult it would be to develop 50 different frameworks based on state law. At the same time, we want to ensure that states play a role in protecting the privacy of their residents.

What should, in your view, be the role of State AGs in enforcing privacy standards?

Answer. We believe that the Federal Trade Commission ("FTC") is the appropriate agency to oversee and enforce online privacy and data security. The FTC is the Nation's leading agency when it comes to privacy enforcement, having brought hundreds of privacy and data security cases. Importantly, it has broad authority to safeguard consumers and enforce privacy protections across the entire online ecosystem—reflecting the principle of "parity" which we believe is essential to an effective privacy framework. We are open to discussing a role for State AGs in enforcing a national framework, but any enforcement mechanism ultimately adopted must be consistent with the principle of national uniformity.

Question 6. Law Enforcement: I believe our law enforcement officials should have a mechanism to obtain the data they need for legitimate investigations. At the same time we need to strike the right balance between keeping our country and communities safe while protecting individuals' civil rights and privacy. Your company has access to many of the personal and intimate choices of millions of your customers, data and records that paint the picture of the everyday lives of millions of American families.

How do you believe a national privacy framework could seek to strike the right balance?

Answer. We believe that the goals of law enforcement and protection of privacy can coexist. We currently offer meaningful privacy protections to our consumers while also responding to legitimate requests from law enforcement through appropriate channels, such as court orders. We are happy to work with the Committee in ensuring the appropriate balance between these important interests as part of a national privacy framework.

Question 7. Privacy Enhancing Technology: There are many technologies that actually enhance users' privacy: Encryption, anti-virus, cybersecurity technologies are all examples of this. I think this is a portion of the privacy debate that sometimes gets looked over, but one we should consider as we look at privacy legislation.

Can you summarize some of the privacy enhancing technology used at your company?

Answer. Charter is committed to protecting the security and integrity of its systems, networks, and databases. We have invested heavily in developing and implementing numerous cybersecurity programs and processes, including risk management programs, security and event monitoring capabilities, detailed incident response plans, and other advanced detection, prevention, and protection capabilities, including practices and tools to monitor and mitigate insider threats. Charter's cybersecurity framework includes utilizing standards recommended in the cybersecurity framework core established by the National Institute of Standards and Technology ("NIST"), which maps the core functions and underlying categories and subcategories to various standards, such as ISO 27001 and others. Charter also continues to evaluate new and more advanced technologies to monitor and mitigate insider threats.

In addition to these cybersecurity measures, the Data Over Cable Service Interface Specification (DOCSIS) standard that Charter uses to deliver Internet access service was built with encryption from the beginning. Today, we utilize Advanced Encryption Standard (AES) 128 to encrypt the data packets traveling over our broadband network so that a customer's broadband usage remains secure.

Finally, Charter makes available to all of its subscribers a Security Suite (*https://www.spectrum.net/security-suite/*) of services that includes advanced real-time protection against viruses, spyware and other malicious attacks; a secure firewall to prevent hacking attempts, keeping private data safe; automatic updates through cloud-based technology; spyware detection and removal; browsing protection that automatically blocks unsafe sites (for computers running Windows); and parental controls to protect children against harmful content (for computers running Windows).

Question 8. Do you believe the Federal Government could assist in either funding the development of similar technologies or establishing a framework for companies to implement them into their data processing?

Answer. Charter believes that the Federal Government can play an important role in promoting advancements in products and services that improve privacy protection, through the establishment of consensus standards such as the NIST

cybersecurity framework. The government should avoid requiring the use of particular technologies or products, however. We believe the most important thing the government can do to promote the development of effective privacy technologies is to establish a uniform national privacy framework that clearly identifies provider obligations and makes those obligations applicable to all participants in the online ecosystem so that consumers are protected regardless of where they go online.

Question 9. Small Business: As we talk about a national framework, one of the most important things to keep in mind is how we work with small business. Your company has the ability to maintain cybersecurity and compliance teams that make it easier for your companies to work with any potential law we pass.

Can you discuss how your companies might be working with, or aiding, small businesses with their privacy and data needs?

Answer. Charter provides services to many small and medium sized businesses ("SMBs"). We provide our SMB subscribers with the same data protections, and follow the same data practices, that we do for our residential subscribers.

Question 10. Also, can you provide your thoughts on how a Federal framework would best take the challenges and opportunities of small businesses into account?

Answer. Customers of small businesses should have the same control over the use and disclosure of their personal information as any other consumers, and the same confidence that their personal information is being protected. Any special rules for small businesses must not result in gaps in privacy protection or create competitive disparities among ecosystem participants.

Question 11. Data Protection Officers: As you all 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 company's perspective on this requirement?

Answer. Charter supports retaining the flexibility for companies to address the issue of privacy in a manner that is consistent with their corporate structure and would be most effective within the context of the individual organization.

Question 12. Data Minimization: One component of the GDPR is a concept known as "data minimization." This principle states that data processing should only use as much data as is required to successfully accomplish a given task and data collected for one purpose cannot be repurposed without further consent. The idea behind this is both to ensure that users are comfortable that their data is only being used for the purposes which enhance the experience and also help limit the impact of any data breaches.

It seems like there may be challenges to implementing something this broad, especially as it is laid out in the GDPR, but it nonetheless feels like something that should be explored as part of our conversation here in the United States.

What is your company's perspective on this requirement?

Answer. Charter believes that data minimization is one option among a menu of privacy principles that can help to safeguard and protect consumer privacy. Data minimization is inherently linked to consumer control and choice. Charter's proposed opt-in approach to consumer privacy would minimize the amount of data collected by increasing consumer control over the collection and use of their personal online information. We look forward to working with you and the Committee on this and other approaches for achieving this objective.

Question 13. 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.

Do you build your own data centers or contract with another entity?

Answer. Charter both owns data centers and contracts for storage of data with third parties.

Question 14. What steps do you take to secure these centers?

Answer. Charter is committed to protecting the security and integrity of its systems, networks, and data. For the servers that Charter owns, we have invested heavily to develop and implement numerous cybersecurity programs and processes, including risk management programs, security and event monitoring capabilities, detailed incident response plans, and other advanced detection, prevention, and protection capabilities, including practices and tools to monitor and mitigate insider

threats. For data stored on third-party servers, our contracts include the provision of security by the host.

Question 15. How often to you review your physical data security standards at your data centers?

Answer. Charter routinely reviews its security technologies and practices to confirm they are sufficient to protect our systems, networks, and data. We also routinely conduct information technology security audits of our vendors, as well as periodic reviews of their security practices.

○