

**POLICY PRINCIPLES FOR A FEDERAL DATA
PRIVACY FRAMEWORK IN THE UNITED STATES**

HEARING

BEFORE THE

**COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE**

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

—————
FEBRUARY 27, 2019
—————

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



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

—————
U.S. GOVERNMENT PUBLISHING OFFICE

60-880 PDF

WASHINGTON : 2025

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ROGER WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota	MARIA CANTWELL, Washington, <i>Ranking</i>
ROY BLUNT, Missouri	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	RICHARD BLUMENTHAL, Connecticut
DEB FISCHER, Nebraska	BRIAN SCHATZ, Hawaii
JERRY MORAN, Kansas	EDWARD MARKEY, Massachusetts
DAN SULLIVAN, Alaska	TOM UDALL, New Mexico
CORY GARDNER, Colorado	GARY PETERS, Michigan
MARSHA BLACKBURN, Tennessee	TAMMY BALDWIN, Wisconsin
SHELLEY MOORE CAPITO, West Virginia	TAMMY DUCKWORTH, Illinois
MIKE LEE, Utah	JON TESTER, Montana
RON JOHNSON, Wisconsin	KYRSTEN SINEMA, Arizona
TODD YOUNG, Indiana	JACKY ROSEN, Nevada
RICK SCOTT, Florida	

JOHN KEAST, *Staff Director*

CRYSTAL TULLY, *Deputy Staff Director*

STEVEN WALL, *General Counsel*

KIM LIPSKY, *Democratic Staff Director*

CHRIS DAY, *Democratic Deputy Staff Director*

RENAE BLACK, *Senior Counsel*

CONTENTS

	Page
Hearing held on February 27, 2019	1
Statement of Senator Wicker	1
Prepared statement	3
Statement of Senator Cantwell	4
Prepared statement	5
Statement of Senator Fischer	51
Statement of Senator Klobuchar	52
Statement of Senator Thune	54
Statement of Senator Schatz	57
Statement of Senator Moran	59
Statement of Senator Markey	60
Statement of Senator Blackburn	62
Statement of Senator Blumenthal	64
Statement of Senator Capito	65
Statement of Senator Rosen	67
Statement of Senator Lee	68
Statement of Senator Baldwin	70
Statement of Senator Young	72
Statement of Senator Cruz	74
WITNESSES	
Jon Leibowitz, Co-Chairman, 21st Century Privacy Coalition	6
Prepared statement	8
Michael Beckerman, President and Chief Executive Officer, Internet Association	11
Prepared statement	12
Brian Dodge, Chief Operating Officer, Retail Industry Leaders Association	21
Prepared statement	23
Victoria Espinel, President and Chief Executive Officer, BSA The Software Alliance	27
Prepared statement	29
Randall Rothenberg, Chief Executive Officer, Interactive Advertising Bureau	34
Prepared statement	36
Dr. Woodrow Hartzog, Professor of Law and Computer Science, Northeastern University School of Law and Khoury College of Computer Science	39
Prepared statement	41
APPENDIX	
Response to written questions submitted to Jon Leibowitz by:	
Hon. Jerry Moran	77
Hon. Marsha Blackburn	78
Response to written questions submitted to Michael Beckerman by:	
Hon. Jerry Moran	78
Hon. Cory Gardner	82
Hon. Marsha Blackburn	83
Response to written questions submitted by Hon. Jerry Moran to:	
Brian Dodge	83
Randall Rothenberg	85

**POLICY PRINCIPLES FOR A FEDERAL DATA
PRIVACY FRAMEWORK IN THE
UNITED STATES**

WEDNESDAY, FEBRUARY 27, 2019

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

The Committee met, pursuant to notice, at 10 a.m. in room SH-216, Dirksen Senate Office Building, Hon. Roger Wicker, Chairman of the Committee, presiding.

Present: Senators Wicker [presiding], Thune, Cruz, Fischer, Moran, Sullivan, Gardner, Blackburn, Capito, Lee, Johnson, Cantwell, Klobuchar, Blumenthal, Schatz, Markey, Peters, Baldwin, Tester, and Rosen.

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

The CHAIRMAN. This hearing will come to order. Good morning to you all. Today we hold our first hearing this Congress to discuss policy principles for a Federal consumer data privacy framework. I am glad to convene this hearing with my good friend Ranking Member Cantwell. We live during an exciting time of rapid innovation and technological change. Internet connected devices and services are virtually everywhere—in our homes, cars, groceries stores, and right here in our pockets. The increase in Internet connected devices and services means that more consumer data than ever before is flowing through the economy.

The economic and societal benefits generated by the consumer data are undeniable. From this data, meaningful insights are gleaned about the needs, preferences, and demands of consumers and businesses alike. These insights spur innovation, help target investment, and create opportunities. The material benefits of data include increased productivity and efficiency, reduced costs, greater efficiency, greater convenience, and access to customized goods and services that enhance our safety, security, and overall quality of life.

While the benefits of consumer data are immense, so too are the risks. Consumer data in the digital economy has become a target for cybercriminals and actors that exploit data for nefarious purposes. This problem is exacerbated by the failure of some companies to protect consumer data from misuse and unwanted collection and processing. These issues threaten to undermine consumers' trust in the Internet marketplace, diminishing consumer engage-

ment in the online ecosystem. Consumer trust in the Internet marketplace is essential. It is a driving force behind the ingenuity and success of American technological advancement and prosperity.

Congress needs to develop a uniquely American data privacy framework that provides consumers with more transparency, choice, and control over their data. This must be done in manner that provides for continued investment and innovation, and with the flexibility for U.S. businesses to compete domestically and abroad. It is clear that we need a strong, national privacy law that provides baseline data protections, applies equally to business entities both online and offline, and is enforced by the Nation's top privacy enforcement authority, the Federal Trade Commission.

It is important to note that a national framework does not mean a weaker framework than those that have already passed in the U.S. and overseas or being contemplated in the various States. Instead it means a preemptive framework that provides consumers with certainty that they will have the same set of robust data protections no matter where they are in the United States.

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

I hope our witnesses will address the critical issues that this committee will need to consider in developing a Federal data privacy law, including how best to protect consumers' personal data from being used in ways they did not consent to when collected by the stores or websites they visit. How to ensure that consumers are presented with simplified notices about what information an organization collects about them instead of lengthy and confusing privacy notices or terms of use that are often written in legal ease and bury an organization's data collection activities. How to enhance the FTC's authority and resources in a reasonable way to police privacy violations and take action against bad actors anywhere in the ecosystem. How to create a framework that promotes innovation and values the significant contributions of entrepreneurs, startups, and small businesses to the U.S. economy. How to provide consumers with certainty about their rights to their data, including the right to access, correct, delete and port their data while maintaining the integrity of business operations and avoiding unnecessary disruptions to the Internet marketplace. And how to ensure a United States data privacy law is interoperable with international laws to reduce compliance burdens on U.S. companies with global operations.

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

[The prepared statement of Senator Wicker follows:]

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

Good morning to you all. Today we hold our first hearing this Congress to discuss policy principles for a Federal consumer data privacy framework. I am glad to convene this hearing with my good friend, Ranking Member Cantwell.

We live during an exciting time of rapid innovation and technological change. Internet-connected devices and services are virtually everywhere—in our homes, cars, grocery stores, and right here in our pockets.

The increase in Internet-connected devices and services means that more consumer data than ever before is flowing through the economy.

The economic and societal benefits generated by the consumer data are undeniable. From this data, meaningful insights are gleaned about the needs, preferences, and demands of consumers and businesses alike. These insights spur innovation, help target investment, and create opportunities.

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

While the benefits of consumer data are immense, so too are the risks.

Consumer data in the digital economy has become a target for cyber-criminals and actors that exploit data for nefarious purposes.

This problem is exacerbated by the failure of some companies to protect consumer data from misuse and unwanted collection and processing.

These issues threaten to undermine consumers' trust in the Internet marketplace, diminishing consumer engagement in the online ecosystem.

Consumer trust in the Internet marketplace is essential. It is a driving force behind the ingenuity and success of American technological advancement and prosperity.

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

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

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

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

We welcome our distinguished witness panel:

- Mr. Michael Beckerman, President and CEO of the Internet Association
- Mr. Brian Dodge, Chief Operating Officer of the Retail Industry Leaders Association
- Ms. Victoria Espinel, President and CEO of BSA | The Software Alliance
- Mr. Jon Leibowitz, Co-Chairman of the 21st Century Privacy Coalition
- Mr. Randall Rothenberg, CEO of the [Interactive] Advertising Bureau
- Dr. Woodrow Hartzog, Professor of Law and Computer Science at Northeastern University School of Law and Khoury College of Computer Sciences

I hope our witnesses will address the critical issues that this committee will need to consider in developing a Federal data privacy law, including:

- How best to protect consumers' personal data from being used in ways they did not consent to when collected by the stores or websites they visit.
- How to ensure that consumers are presented with simplified notices about what information an organization collects about them, instead of lengthy and confusing privacy notices or terms of use that are often written in legalese and bury an organization's data collection activities.
- How to enhance the FTC's authority and resources in a reasonable way to police privacy violations and take action against bad actors anywhere in the ecosystem.
- How to create a framework that promotes innovation and values the significant contributions of entrepreneurs, start-ups, and small businesses to the U.S. economy;

- How to provide consumers with certainty about their rights to their data—including the right to access, correct, delete, and port their data, while maintaining the integrity of business operations and avoiding unnecessary disruptions to the Internet marketplace; and
- How to ensure a United States data privacy law is interoperable with international laws to reduce compliance burdens on U.S. companies with global operations.

I look forward to a thoughtful discussion on these issues and I want to welcome all of our witnesses and thank them for testifying this morning.

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

Senator CANTWELL. Thank you, Mr. Chairman, and thank you for holding this important hearing. And welcome to the witnesses today as we discuss moving forward on developing a Federal data privacy framework. Last year we learned that political consulting firm, Cambridge Analytica, gained unauthorized access to personal information of 87 million Facebook users, which it used for profiling purposes. That same year, Uber announced that hackers had successfully gained access to the personal information of 57 million riders and drivers.

The year before, in 2017, hackers successfully stole the personal information of 143 million consumers from Equifax because the credit reporting giant failed to install a simple software patch. And just last week, UConn Health announced that an unauthorized, third-party access to employee e-mail accounts potentially exposing personal and medical information of approximately 326,000 people. These are not isolated incidents or even one-offs. They are the only latest in a barrage of consumer privacy and security violations, many of which are entirely preventable. And consumers are at the receiving end of this reckless practice. So, I hope that Congress does grapple with Federal privacy data legislation.

While Congress has been successful in the past in addressing certain types of personal information, such as health or financial data or children's information, consumers continue to see the challenges that they face with corporate practices that allow for collections, storage, analyzing, and monetizing their personal information. In fact, just 2 years ago, Congress voted to overturn the FCC privacy rule that would have protected online users from Internet service providers but had yet to take effect. So, while we have gone backward in some ways, there are others who are moving forward. In May 2018, the European's General Data Privacy Regulations went into effect, providing the E.U. and its citizens with array of new protections from certain types of corporate data practices.

And in addition, the State of California has recently passed the California Consumer Privacy Act, which also provided California citizens with new rights and protections. And this law goes into effect in 2020. So together, the implementation of these two pieces of legislative policy, GDPR and CCPA, have brought new insights to the Congressional efforts to pass meaningful privacy and data security laws. What is clear to me is we cannot pass a weaker Federal law just at the expense of States. So, Mr. Chairman, I am certainly open to exploring the possibility of meaningful, comprehensive, Federal privacy legislation.

I want to work with you and all the members of this committee, many of which who have already introduced various pieces of privacy legislation for thoughtful discussion about how we come to a resolution on these issues. I do not think anyone should be under the illusion though that this is an easy task. The information age is still unfolding. The many challenges that we will face as new ways that information is shared, cannot just simply be decided today. There are hard issues about how this economy will evolve, but I know that we can have a thoughtful exploration of the multifaceted issues regarding Federal policy that go beyond the stalemate that we have had for several years.

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

So, at today's hearing, I hope we kick off a very substantive discussion to explore how we go about changing this mindset that treats personal information as such a commodity for profit, and think about it, as we have, in tackling a series of hearings here, Mr. Chairman, on the various issues related to consumer privacy and security. I know that there are members of both sides of the aisle who are very committed to this cause, and I hope we can make progress on this.

Thank you, Mr. Chairman.

[The prepared statement of Senator Cantwell follows:]

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

Thank you, Mr. Chairman. And thank you for holding this important hearing and welcome to the witnesses today as we discuss moving forward on developing a Federal data privacy framework.

Last year, we learned that political consulting firm Cambridge Analytica gained unauthorized access to personal information of 87 million Facebook users, which it used for profiling purposes. That same year, Uber announced that hackers had successfully gained access to the personal information of 57 million riders and drivers. The year before, in 2017, hackers successfully stole the personal information of 143 million consumers from Equifax because the credit reporting giant failed to install a simple software patch. And just last week, UConn Health announced that an unauthorized 3rd party accessed employee e-mail accounts, potentially exposing personal and medical information of approximately 326,000 people.

These are not isolated incidents, or even one-offs. They are the latest in a barrage in consumer privacy and security violations, many of which are entirely preventable. And consumers are at the receiving end of this reckless practice. So, I hope that Congress does grapple with privacy data legislation.

While Congress has been successful in the past in addressing certain types of personal information, such as health or financial data or children's information, consumers continue to see the challenges that they face with corporate practices that allow for collection, storage, analyzing, and monetizing their personal information. In fact, just two years ago, Congress voted to overturn the FCC privacy rule that would have protected online users from Internet service providers, but had yet to take effect.

So, while we have gone backwards in some ways, there are others who are moving forward. In May of 2018, the European's General Data Privacy Regulations went into effect, providing the EU and its citizens with an array of new protections from certain types of corporate data practices. And in addition, the state of California has recently passed the California Consumer Privacy Act, which also provided California's citizens with new rights and protections. This law goes into effect 2020.

So, together the implementation of these two pieces of legislative policy, GDPR and CCPA, have brought new insights to the congressional efforts to pass meaning-

ful privacy and data security laws. What is clear to me is we cannot pass a weaker Federal law at the expense of states.

So, Mr. Chairman, I am certainly open to exploring the possibility of meaningful, comprehensive Federal privacy legislation. I want to work with you and all the members of this committee, many of which have already introduced various pieces of privacy legislation, for thoughtful discussion about how we come to a resolution on these issues.

I don't think anyone should be under the illusion, though, that this is an easy task. The information age is still unfolding. The many challenges that we will face as new ways that information is shared cannot just simply be decided today. There are hard issues about how this economy will evolve. But, I know that we can have a thoughtful exploration of the multifaceted issues regarding Federal policy that go beyond the stalemate that we have had for several years. If we are going to deliver meaningful privacy and security protection for the deserving American public, then we must think about what this paradigm really looks like in this debate. I believe that just notice and consent are no longer enough. I don't think that transparency is the only solution.

So, at today's hearing, I hope we kick off a very substantive discussion to explore how we go about changing this mindset that treats personal information as such a commodity for profit, and think about it as we have in tackling a series of hearings here, Mr. Chairman, on the various issues related to privacy and security. I know that there are members on both sides of the aisle that are very committed to this cause, and I hope we can make progress on this.

Thank you Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator Cantwell. We now welcome our distinguished witnesses, and we will just start at this end of the table with Mr. Leibowitz. We ask each witness to limit opening remarks to 5 minutes. Mr. Leibowitz, thank you, sir.

**STATEMENT OF JON LEIBOWITZ, CO-CHAIRMAN,
21ST CENTURY PRIVACY COALITION**

Mr. LEIBOWITZ. Thank you so much, Mr. Chairman and Ranking Member Cantwell, other members of the Committee. Appreciate your inviting me to testify today on behalf of the 21st Century Privacy Coalition.

To begin, let me state unequivocally, the Coalition, which is composed of the Nation's leading telecommunications companies, supports strong Federal privacy legislation that gives consumers more control over their data. It is the right thing to do for all Americans. And we want to commend this committee, and particularly Chairman Wicker and Senators Blumenthal, Moran, and Schatz, for the thoughtful bipartisan work you have done to move that process along. Simply put, Americans deserve meaningful privacy protections that give them the right to decide how their personal information is used and shared.

The passage of privacy laws in Sacramento, in Brussels, has demonstrated that elected officials can enact privacy protections. Now you can demonstrate that same commitment for Americans, but you can do it better. Mr. Chairman, to get privacy right, we believe the best place to start is the landmark 2012 FTC privacy report, which I brought with me today. During my time at the agency, we thought a lot about the best statutory design for protecting privacy, and after more than 2 years based on decades of privacy enforcement, we produced a framework praised by privacy advocates, for its muscular approach to protecting privacy. And the principles embodied in that report remain the centerpiece of the FTC's privacy regime today. Here is what that report called for, greater consumer control over data, more transparency, privacy by

design, opt-in rights for sensitive information, opt-out rights for non-sensitive information, rights of access and deletion where appropriate, and a comprehensive technology-neutral framework. And these are all ideas, by the way, that were also supported by the Obama Administration. Why? Because privacy should not be about who collects consumer data, it should be about what data is collected and how it is protected.

Strong protection should be backed up by strong enforcement authority for the FTC, America's top privacy cop. Congress should provide my former agency with the ability to impose civil penalties for violators for first offenses, so malefactors do not get a second bite at the consumer deception apple, as well as additional resources to support its mission. And perhaps, some APA rulemaking that could be with guardrails. We also recognize that the States have an important role to play in protecting privacy, which is why Attorneys General should have the authority to enforce any new Federal privacy law. In addition to being the right thing to do, Mr. Chairman, enacting Federal privacy legislation is necessary in light of the patchwork of privacy bills being produced in legislators around the Country. That is because what makes the Internet magical is also what makes it a poor subject for State legislation. It connects individuals across State lines. Imagine if there were 50 different FAA standards, one for every State. The inevitable confusion could cause disastrous consequences in the air. Well, the confusion caused when consumers try to navigate through 50 States' cyberspace standards, could cause digital disasters as well and, at the very least, consumer confusion.

What's more, in their rush to address the need for stronger privacy protections, State lawmakers are drafting, and sometimes passing, legislation in haste. California's law puts tough tech-neutral limits on the sale of information and heighten restrictions on children's information, but the law also suffers from multiple drafting flaws. For example, it defines personal information based on households, when we all know that different people living under the same roof can have very different privacy preferences. And notably, California State lawmakers preempted their own municipal privacy legislation—regulations. A bill being considered in Washington State is promising but also not problem-free. Indeed Mr. Chairman, there are currently 94 privacy proposals pending in State capitals. 94 involving various and differing regulatory schemes. The unintended consequences of these efforts do not just fall on large corporations, they hit small businesses, they stifle innovation, they balkanize commerce.

Mr. Chairman, as you know, preemption in its best form is taking the most successful aspects of State policies and making them part of a regime that benefits everyone. For these reasons, the 21st Century Privacy Coalition's view is that you should pass strong, national privacy law—a strong, national privacy law based on the FTC framework that gives consumers more control over their data, provides greater transparency, and allows enforcers to sanction any digital gangsters who abuse the public trust.

Thank you.

[The prepared statement of Mr. Leibowitz follows:]

PREPARED STATEMENT OF JON LEIBOWITZ, CO-CHAIR,
21ST CENTURY PRIVACY COALITION

“AMERICA’S PRIVACY MOMENT: THE NEED FOR STRONG FEDERAL PRIVACY
PROTECTIONS THAT GIVE CONSUMERS MORE CONTROL OVER THEIR DATA”

Chairman Wicker, Ranking Member Cantwell, and other distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing examining policy principles for a Federal data privacy framework. My name is Jon Leibowitz and I am a partner at the law firm of Davis Polk & Wardwell LLP. I also serve as co-chair of the 21st Century Privacy Coalition. During my time in government, I served as a Democratic Commissioner (2004–2009) and Chairman (2009–2013) of our Nation’s leading consumer privacy enforcement agency, the Federal Trade Commission (“FTC”).¹

There is a growing consensus both inside the halls of Congress and across America that Federal privacy legislation is necessary to bolster consumer confidence in the privacy practices of online services, which in turn is necessary to foster continued U.S. innovation and leadership in the Internet ecosystem and the broader information-based economy. For those reasons and because it is the right thing to do, members of the 21st Century Privacy Coalition enthusiastically support Federal legislation that provides stronger and more meaningful privacy protections for American consumers. We also want to commend this Committee, particularly Chairman Wicker and Senators Blumenthal, Moran, and Schatz, for its leadership on this important issue of intense public concern.

The 21st Century Privacy Coalition is composed of the Nation’s leading communications companies, which have a significant interest in fortifying consumer trust in online services and confidence in the privacy and security of their personal information.² We are supporters of strong consumer privacy rights and firmly believe that companies must provide transparency to consumers, disclose what consumer data is being collected and how it is being used, manage consumer data in a responsible manner,³ and be held accountable for honoring their commitments to consumers. For decades, our companies have adhered to enforceable, robust privacy principles through practices that safeguard consumer data based on the key tenets of the bipartisan FTC privacy regime as outlined in the Commission’s landmark Privacy Report.⁴ We continue to adhere to such policies today.

Companies like ours that have always had vigorous privacy programs in place know that a uniform national privacy law would be good for the Internet economy. Last month, the Government Accountability Office (“GAO”), based on a request by House Energy & Commerce Chairman Pallone, produced its own report encouraging Congress to consider enacting a comprehensive Internet privacy law.⁵ Our members welcome legislation that requires all marketplace participants to start from a place of transparency, security, control, and rights for American consumers.

A Federal Solution Is Critical

We strongly believe that Congress needs to enact national privacy legislation that gives consumers statutory rights to control how their personal information is used and shared; provides increased visibility into companies’ practices when it comes to managing consumer data; and includes an opt-in consent regime for the use and sharing of customers’ sensitive personally identifiable information—including health and financial information, precise geo-location information, social security numbers, and children’s information—consistent with the framework articulated by the FTC

¹The FTC has brought hundreds of privacy and data security cases, including many against companies for misusing or failing to reasonably protect consumer data, almost always with unanimous votes from its Commissioners.

²The member companies/associations of the 21st Century Privacy Coalition are AT&T, CenturyLink, Comcast, Cox Communications, CTIA, NCTA—The Internet and Television Association, T-Mobile, USTelecom, and Verizon.

³The 21st Century Privacy Coalition has also long supported strong Federal data security legislation. See, e.g., *Discussion Draft of H.R., Data Security and Breach Notification Act of 2015: Hearing Before the Subcomm. on Commerce, Manufacturing, & Trade of the H. Comm. on Energy & Commerce*, 114 Cong. 59–67 (2015) (statements of Jon Leibowitz, Co-chair, 21st Century Privacy Coalition).

⁴See FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), available at: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁵See Government Accountability Office, *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility* (Jan. 2019), available at: <https://www.gao.gov/assets/700/696437.pdf>, at 37.

in its Privacy Report. The recommendations in the Privacy Report, which were lauded by the privacy community for their muscular approach to consumer protection, were based on institutional expertise accrued over decades, through hundreds of cases brought by the FTC against companies to ensure privacy and security of consumer information, as well as from the input of dozens of stakeholders (including businesses, privacy advocates, and academics), and multiple consumer privacy and data security workshops.

The FTC also recognized—and we hope you would agree—that privacy should not be about *who* collects an individual’s personal information, but rather should be about *what* information is collected and *how* it is protected and used. That is why we firmly believe that Federal privacy legislation should be technology- and industry-neutral.

Companies that collect, use, or share the same type of personal information should not be subject to different privacy requirements based on how they classify themselves in the marketplace. As an extensive survey by the Progressive Policy Institute conclusively found, consumers (1) overwhelmingly (*i.e.*, 94 percent) want the same privacy protections to apply to their personal information *regardless* of the entity that collects such information; and (2) overwhelmingly (83 percent) expect to enjoy heightened privacy protections for sensitive information and for uses of their sensitive information that present heightened risk of consumer harm, again *regardless* of the company charged with maintaining it.⁶

The optimal approach would provide consumers with easy-to-understand privacy choices based upon the nature of the information itself—its sensitivity, and the risk of consumer harm if such information is the subject of an unauthorized disclosure—and the context in which it is collected. For example, consumers expect sensitive information about their medical histories, financial status, and Social Security numbers to receive heightened protection to ensure confidentiality. A sensitivity- and risk-based approach imposes less stringent requirements on *non*-sensitive information and information that is de-identified or anonymized because of the lower risk that consumers would be harmed, or even that such information could be associated with an individual.

Accordingly, a national privacy law based on the FTC’s Privacy Report would best promote consumer control and choice by imposing requirements for obtaining meaningful consent based on the risks associated with different kinds of data and different uses of data. That approach should include clear consumer controls such as opt-in rights for sensitive information, opt-out rights for non-sensitive information, and inferred consent for certain types of operational uses of information by companies (such as in the case of order fulfillment, fraud prevention, and some forms of first-party marketing). We also believe that consumers should have certain rights of access and deletion where appropriate.

A privacy law must also recognize that different consumers have different privacy preferences. One of the most remarkable things about the Internet is that it allows us to tailor our use to our own needs and interests. We agree with the GAO that Congress must carefully consider the balance between the need for consumer privacy protections and companies’ ability to provide and improve the services on which we have come to expect and depend.⁷ Legislation should not limit consumer choice by inhibiting consumer-friendly incentive programs tied to privacy choices such as rewards programs. Rather, the law should require companies to have a privacy policy that gives consumers clear and comprehensible information about the categories of data that are being collected, used, or shared, and the types of third parties with which information may be shared. So long as consumers are provided with information about the nature of such programs, they should be allowed to make their own choices.

⁶See Memorandum from Public Opinion Strategies and Peter D. Hart to the Progressive Policy Institute, Key Findings from Recent National Survey of Internet Users (May 26, 2016), <https://www.progressivepolicy.org/wp-content/uploads/2016/05/Internet-User-National-Survey-May-23-25-Key-Findings-Memo.pdf> (finding that 94 percent of consumers favor such a consistent and technology-neutral privacy regime, and 83 percent of consumers say their online privacy should be protected based on the sensitivity of their online data, rather than by the type of Internet company that uses their data). See also <https://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rules-protecting-information/> (“Ultimately, consumers want to know there is one set of rules that equally applies to every company that is able to obtain and share their data, whether it be search engines, social networks, or ISPs, and they want that data protected based on the sensitivity of what is being collected” said Peter Hart.”).

⁷GAO Report, at 38.

A Problematic Patchwork: Avoiding Inconsistent State Laws

Strong privacy protections need to apply to consumers regardless of where in the United States they live, work, or happen to be accessing information. By its very nature, the Internet connects individuals across state (and international) lines. Put simply, data knows no state boundaries.

For this reason, state intervention in this quintessentially interstate issue is problematic, no matter how well-intentioned it may be. A proliferation of different state privacy requirements would create inconsistent privacy protections for consumers. A Mississippi wireless customer visiting Connecticut should not have different privacy protections than a Connecticut wireless customer visiting Mississippi. Nor should a Kansas resident enjoy different privacy protections when at work just over the border on the Missouri side of Kansas City, or a Hawaii resident when traveling to any of the contiguous U.S. states.

Thus, the absence of a national privacy law yields inconsistent protections and consumer confusion about the scope of their privacy protections and the jurisdictions in which such protections apply. In addition, the proliferation of state and local consumer privacy laws in place of a national framework creates significant compliance and operational challenges for businesses of all sizes. It also erects barriers to the kind of innovation and investment that is a lifeblood of our Nation's economy, and to many beneficial and consumer-friendly uses of information.

Ensuring Enforcement

But preempting state laws should not mean weakening protections for consumers. A Federal consumer privacy law needs to be a strong one. We believe that the Members of this Committee understand that, and we encourage all stakeholders to come together to develop such a Federal law. Blanket opposition to preemption of state legislation offers no protection to consumers. Congress should be able to develop a law that guarantees strong privacy rights to consumers in—and adopts the best practices from the laws of—every state. And the Coalition believes states as well as the FTC have a critical role to play in enforcing those rights.

The FTC should have the primary authority to enforce a national privacy law. Our nation's top consumer protection agency has brought more than 500 cases to protect the privacy and security of consumer information, including those against large companies like Facebook, Google, Twitter, Uber, Dish Network, and others. To support the agency in its mission, Congress should provide the FTC with the ability to impose civil penalties on violators for first offenses. We also recognize that the FTC may have a role to play in developing rules to address certain details that Congress may not be able to tackle in the legislation itself, although the boundaries of any such authority should be clear in the legislative text. And we strongly support Congress providing the agency with additional resources necessary to undertake appropriate enforcement actions to keep all companies honest and compliant.

While we believe Federal legislation, rather than a state-by-state approach, should be enacted to ensure consistent, understandable, and robust consumer privacy rights, we also recognize that state attorneys general are critical allies in the realm of consumer protection. They should also be given the power to enforce any new Federal law.

A consumer privacy law, though, should not include criminal penalties or private rights of action, which often result in class actions that primarily benefit attorneys while providing little, if any, relief to actual victims. Private rights of action also frequently result in the diversion of company resources from compliance to litigation, which ultimately does not help consumers who, at the end of the day, simply want companies to follow the law. Providing the FTC and state AGs with enforcement power backed up with civil fining authority provides a far better approach for consumers, as evidenced by its success in policing violations of children's privacy through the Children's Online Privacy Protection Act.

Conclusion

Thank you again for the opportunity to testify today. The 21st Century Privacy Coalition looks forward to working with all Members of the Committee and all stakeholders to craft strong national privacy legislation. As Americans' online and offline activity involving personal information continues to grow in size and scope, consumers across the country deserve a clear understanding of how their personal information is being used and shared, and what is being done to protect their data from hackers and other bad actors.

The United States would benefit significantly from a unified, technology-and industry-neutral Federal privacy law that applies uniformly to all entities, regardless of their business model. And new Federal legislation that preempts other state and Federal requirements would eliminate the consumer confusion and frustration, busi-

ness uncertainty, and other debilitating effects such as reduced investment and innovation resulting from multiple and likely inconsistent regimes applying to the same information. Such a Federal law would provide the greatest clarity and certainty about the rights of consumers and the responsibilities of companies that collect, use, or share consumers' personal information.

We encourage Congressional action that recognizes the yet-untapped potential of both the online world and the increasingly digitized offline world, while providing Americans with the confidence that they will be safe when taking advantage of all these frontiers have to offer.

The CHAIRMAN. And thank you very much, Mr. Leibowitz. Mr. Beckerman with the Internet Association. You are recognized for 5 minutes, sir.

**STATEMENT OF MICHAEL BECKERMAN, PRESIDENT AND
CHIEF EXECUTIVE OFFICER, INTERNET ASSOCIATION**

Mr. BECKERMAN. Thank you, sir. Chairman Wicker, Ranking Member Cantwell, members of the Committee, thank you for inviting me to testify today. My name is Michael Beckerman. I am the President and CEO of the Internet Association, which represents over 45 global Internet companies. Our members include enterprise and consumer-facing businesses that vary in size and business model. I ask my full written testimony and Internet Association's detailed privacy principles be submitted for the record.

The CHAIRMAN. Without objection.

Mr. BECKERMAN. The Internet creates unprecedented benefits for society, and I am here today to discuss why enacting state-of-the-art privacy legislation that protects all Americans in a meaningful way across industries, across technologies, from coast to coast, both on and offline, is in the best interest of consumers. People want and expect more, and we will deliver.

Let me be crystal clear, enacting a nationwide, modernized U.S. privacy framework that provides people meaningful control over their data across all industries, on and offline, is the top priority for our members, and is imperative for the future of our economy and society. We support getting this kind of legislation to the President's desk and signed into law this year. The Internet industry and our member companies are far from perfect. We fail and succeed based on people's trust and we need to do better. We do not always get it right. We have made mistakes. We own up to them, and we are using these challenges as an opportunity to improve. That commitment to improve is driven by the top executives at all of our companies and supported by the employees, engineers, and the entire teams. We can always do better and if you look at the transparency and tools that exist online today, you can see that commitment and improvements that we are making on a daily basis to do better for customers.

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

trust through meaningful transparency, control, accountability, and enforcement. People should have access and control of their data and be able to move, correct, and delete personal information, but the burden should not solely lie on individuals.

Many foreign governments come through the American innovation hubs that we have across the country in every State to better understand the magic behind our industry in order to replicate it in their countries. Today, 7 of the top 10 Internet companies in the world were founded here in the United States. That is something that is worth protecting, enabling, and being proud of. The Internet is one of our great American exports. Internet Association also has traveled around the country and visited States, many of your States as well, and we heard directly from small business owners and community leaders who use data and Internet platforms to grow their business, communicate with customers, and bring the community closer together, and hire new employees. These are the real winners of a data-driven community.

It is important to note that non-tech, small businesses in every State, city, town, and community across the country have the most to lose if we get this legislation wrong, or if we end up with a patchwork of State laws. Data has revolutionized every part of our economy in our daily life. It allows easy access to stay in touch with loved ones from a distance, to get to work on time with efficient navigation, to find the perfect playlist based on curated recommendations, and build communities around shared interests. Data also enables companies to find you better products, show you more relevant content, and get you answers you need quicker. But even with the positive benefits, people have the right to know who is using their data and how. There should be no surprises. This needs to hold true not only for the companies that have a direct relationship with customers on and offline, but also for the thousands of businesses that maybe you have never even heard of that have and use your data without your knowledge.

Specifics that we are supporting are in my written testimony, but speaking very broadly as I wrap up, this law should create one uniform standard that gives individuals control, makes companies accountable, and includes meaningful enforcement. People should have access to the data they share. Be able to move, correct, and delete it when it is not necessary for a service, and there should never be a surprise about who has your data or how it is being used.

In closing, the Internet industry is one of the most customer-centric industries in the world, and while we are already taking tangible steps to provide privacy tools and protections for people in the U.S. and around the world, we are also committed to working with members of this committee and other stakeholders to get meaningful privacy legislation signed as a law.

Thank you.

[The prepared statement of Mr. Beckerman follows:]

PREPARED STATEMENT OF MICHAEL BECKERMAN, PRESIDENT AND CEO,
INTERNET ASSOCIATION

Chairman Wicker, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to testify. My name is Michael Beckerman and I am

President and CEO of Internet Association, which represents over 45 global leading Internet companies.¹ Our members include enterprise and consumer-facing businesses that vary in size and business model. Internet Association's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. The Internet creates unprecedented benefits for society and the economy, and as the voice of the world's leading Internet companies, we ensure stakeholders understand and can take advantage of all the benefits the Internet has to offer.

We appreciate the Committee holding this hearing to advance the conversation around an American approach to data privacy. Internet Association members support a modernized U.S. privacy framework that provides people meaningful control over their data across all industries, makes companies accountable, and includes meaningful enforcement. A globally respected American regulatory framework must prioritize protecting individuals' personal information and foster trust through meaningful transparency and control. We believe this can be done by empowering people to better understand and control how personal information they share is collected, used, and protected. People should also be able to access, correct, move, and delete their personal information except where there is a legitimate need or legal obligation to maintain it. Consumers deserve the right to control the use of their personal information, and we want to see the president sign a new law this year.

The Internet industry and IA member companies are far from perfect. And we understand that we fail or succeed based on people's trust with our products and services. Our members are committed to doing better, and that commitment is driven by the top executives in all of our companies and supported by employees across all parts of the company, including product and technical teams. The transparency² and tools³ that exist online today are a direct result of our industry's commitment to adapting to consumer feedback, and we remain committed to making new improvements every day. People expect more from our industry and we will deliver.

As we consider the important topic of modernizing America's approach to data privacy, it is important to remember that data has revolutionized every part of our economy and daily lives. It allows us to easily stay in touch with loved ones from a distance, get to work on time with efficient navigation, find the perfect playlist based on curated recommendations, and build communities around shared interests. Data also enables farmers to manage their costs of doing business, doctors to provide patients with precision healthcare, and teachers to inform their classroom practices.

Internet Association has travelled around the country and heard directly from small business owners and community leaders who use data and Internet platforms to grow their businesses, communicate with their customers, bring the community together, and hire new employees. We met with a high school sophomore in Shelby, North Carolina who started a local monogram clothing business by taking orders on social media. After two years, demand became so high that she opened a physical store. In Claremont, New Hampshire, we heard from an animal shelter that said animal adoptions tripled since they started posting about their pets online. These are just a few of the millions of stories that exist from non-tech small businesses and nonprofits in every state. These are the real winners of a data-driven community. And if we fail to get this legislation right or end up with a patchwork of state laws, it will be these small businesses that lose out.

The U.S. has long been a global leader in political and technological innovation, empowering our citizens by establishing the world's oldest constitutional democracy, and by investing in the technology that laid the foundation for the Internet as we know it today. We need to develop an approach to privacy legislation that is in keeping with the founding principles of our democracy and the spirit of innovation that underpins America's technological leadership. An American approach to privacy can

¹Internet Association members include Airbnb, Amazon, Ancestry, Coinbase, DoorDash, Dropbox, eBay, Etsy, Eventbrite, Expedia, Facebook, Google, Groupon, Handy, HomeAway, IAC, Intuit, letgo, LinkedIn, Lyft, Match Group, Microsoft, Pandora, PayPal, Pinterest, Postmates, Quicken Loans, Rackspace, Rakuten, reddit, Snap Inc., Spotify, Stripe, SurveyMonkey, Thumbtack, TransferWise, TripAdvisor, Turo, Twilio, Twitter, Uber Technologies, Inc., Upwork, Vivid Seats, Yelp, Zenefits, and Zillow Group.

²For example, <https://transparencyreport.google.com>, <https://transparency.twitter.com>, <https://transparency.facebook.com>, <https://www.linkedin.com/legal/transparency>, <https://help.pinterest.com/en/article/transparency-report>, <https://www.redditinc.com/policies/transparency-report>, <https://www.snap.com/en-US/privacy/transparency/>.

³Examples of privacy tools include: <https://myaccount.google.com/privacycheckup>, <https://www.facebook.com/help/325807937506242>, <https://twitter.com/settings/safety>, <https://www.linkedin.com/psettings/>,

deliver strong, enforceable privacy protections while allowing for continued U.S. leadership in technology.

Internet Association and our member companies are fully committed to supporting the passage of meaningful Federal privacy legislation. We have been active participants in the robust public debate currently taking place in the U.S. around data privacy, and we released Privacy Principles⁴ last year to further the discussion around what an American approach to privacy may look like. We encourage the committee to consider our Privacy Principles as it looks to craft Federal privacy legislation.

All businesses—from search engines to local pizza shops—depend on data to do things like enhance their services, manage inventory, and strengthen relationships with customers. Non-profits also use data to engage their communities, recruit volunteers, and reach new donors. To provide meaningful and comprehensive privacy protections, a Federal privacy law must cover all parts of the economy and eliminate the risk that a confusing patchwork of state laws could impose conflicting obligations on companies that serve customers in multiple states. Americans should have consistent experiences and expectations across state lines and industries—regardless of whether they’re interacting with a company online or offline.

A Federal privacy law should also be grounded in a risk-based approach and avoid overly prescriptive methods that may not be appropriate for all business models. A national framework should consider 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. Not every single piece of data is the same, and it’s important to consider the risks, the harms, and the consequences associated with different types of data.

User trust is fundamental to the success of Internet companies, and responsible data practices are critical for earning and keeping user trust. Any company processing personal data should do so responsibly, acting as a good steward by taking steps to ensure that data is handled in a manner that conforms to consumers’ reasonable expectations. A Federal law can promote the proliferation of responsible data practices by allowing for the use of privacy enhancing techniques such as de-identification or use of aggregated data. California’s new law, in contrast, fails to clearly allow these techniques to be applied to personal information, actually making people less protected.

The Internet industry is among the most consumer-centric industries in the world. Internet companies enable direct, real-time customer interactions and feedback, which help our companies better understand consumers needs to improve and upgrade their services, including on privacy.

Today, with less than five clicks, we can change the privacy settings on our favorite social media site or streaming service. Online platforms also proactively create contextual tools that help us better understand and control our privacy settings. With or without a law, our members will continue listening to their customers and providing them with more control over their data. But, ultimately, we firmly believe that consumers and companies both will benefit from certainty in the rules that govern how data is collected, used, and protected. The burden should not solely lie with individuals.

Individuals Deserve Strong, Unified National Protections

The Internet industry supports a Federal framework that provides all individuals the same fundamental privacy protections regardless of which state they live in, whether they prefer to do business on or offline.

While protections exist today, the current landscape is too complex and disjointed for people to understand. There are privacy laws that impact many aspects of a person’s life, but those laws differ depending on which state they are in, who they share their personal information with, and the type of information they share. There are Federal sectoral protections in the health and financial services areas that apply to certain types of businesses, but don’t protect health and financial information generally. There are laws in some states which give residents of those states protections when dealing with an entity that is covered by the law. Those protections end at the state line. This means that residents of some states benefit from more privacy protections than residents of other states. It also means that residents of a state with privacy protections do not enjoy those protections when they travel, when they purchase from retailers who don’t do business in their state, or when they deal with

⁴https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/

local entities that may not be covered under their state's laws⁵. People should not be expected to know which rules apply depending on where they are and who they are dealing with. IA believes that it is possible to give individuals strong consistent privacy protections while allowing for innovation and economic growth. In fact, we believe that strong consumer privacy laws are critical to the continued success of our industry.

A nationwide standard for the protection of personal information would enhance trust in data uses by providing individuals with a consistent set of expectations that they can rely on in every aspect of their lives. Congress should take action to set an economy-wide privacy standard to ensure individuals have clear expectations in terms of how their personal information will be collected, used, and protected.

There is significant energy in the states to provide new privacy protections to their residents. But this does not solve the complexity issue for individuals or fill all the gaps in privacy protections. In fact, as new privacy laws are passed and come into effect, this landscape becomes more confusing and difficult to understand. State privacy laws are only becoming more splintered, taking widely varying approaches and affording different rights and protections to their residents. This makes it impossible for people, who do not track state privacy legislation as a full-time job, to understand what choices and rights they may have across the different parts of their lives.

IA member companies have heightened awareness of not just the challenges for individuals, but also for businesses that must comply with the patchwork of laws. Most IA members have business models that grow and support small to medium-sized businesses—and know first-hand that compliance burdens fall heaviest on growing businesses that have to devote scarce resources to developing compliance plans to meet each state's requirements.

Federal Privacy Legislation Should Focus On Individual Rights

A Federal privacy law should be centered around the individual in three important respects. First, Federal legislation should ensure that individuals have access to information about the personal information that is collected from or about them, including how that data will be used, shared, and protected. Second, Federal legislation should support the development of tools to give users more control over their personal information. Third, Federal legislation should give individuals the ability to access, delete, correct, and move their personal information.

Transparency

IA's members are leaders in providing users with transparency, granular control, and the ability to exercise rights and choices. IA members have been subject to legal and regulatory obligations to have privacy policies specific to the online environment for years and do the best they can under the current legal framework to ensure their policies are understandable and digestible. FTC enforcement as well as state laws and state attorney general enforcement have built on the requirements for privacy policies. Privacy policies must be carefully written to meet legal requirements and also to avoid enforcement actions if a regulator believes a company has acted in a manner that is inconsistent with their privacy policy. Even though this may naturally end up being the domain of corporate lawyers, IA members have been innovating with privacy policies for years, writing in plain English and making the policies more easily understood. IA member companies create new tools and services, such as privacy centers, that make long policies more modular and easier for users who care about specific issues to quickly find those items and to delve further into details. Many IA members summarize the key elements of their policies at the top and also through short, easy to follow videos. Some member companies also invest in consumer research to determine more effective ways to present information to consumers. All IA members are committed to continuing to improve the ways in which they share information about how data is collected, used, and protected.

Outside the Internet industry, there is still much work to be done to educate people about how their personal information is handled. In some cases, individuals have little to no information about how businesses obtain their personal information, let alone how that information will be used or with whom it may be shared. The lack of a comprehensive Federal privacy law and scattered state laws have left entire industries without any legal requirements to inform consumers about their personal information practices. This cannot continue. Heavily data-driven industries gather personal information from and about individuals, but do so without using the Internet or even direct consumer interaction. The public only finds out about these

⁵ See Cal. Civ. Code § 1798.140(c), which exempts non-profit and small businesses from obligations established by the California Consumer Privacy Act.

businesses' practices when their stores of personal information are the subject of a data breach. Individuals deserve information on who is collecting their information, regardless of the means, and how it is being used. Federal law should shine a light on these practices by requiring entities subject to the law to provide an appropriate level of transparency about data practices.

The inverse of too little information is also problematic for consumers. At the other end of the spectrum, people are overloaded with information that may not be helpful in making important decisions about their privacy. This is particularly true in highly specialized or technical areas where a thorough understanding of the technology infrastructure is necessary to explain in detail how information is collected, the types of information collected, how it may be shared, and the individual's choices about those practices. Though well-intentioned, Europe's new privacy law, the General Data Protection Regulation (GDPR), has exacerbated this problem with new requirements requiring companies to provide even more information. It is not clear that more information benefits EU residents. For example, cookie banner requirements have resulted in consumers being bombarded with notices that in truth offer little choice. A U.S. approach to transparency could show global leadership by developing notice practices that are focused on the desired outcome—individuals understanding the risks and rewards of the use of their data and making informed choices about those risks.

User Control

Once consumers are better informed about data practices, they may want to actively manage the information they share and how it is used. IA's Privacy Principles include the principle that "[i]ndividuals 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." For example, a social networking company may offer different settings for users to control who is able to find their profile or how much information is shared with different types of contacts. On platforms that infer interests from use of the service to make content recommendations or for advertising purposes, providers may share those interests with the user, and allow them to remove interests they no longer want associated with the platform or service. Members who are part of the online advertising ecosystem participate in codes of conduct from the National Advertising Initiative (NAI) and Digital Advertising Alliance (DAA), which give individuals the option to opt-out of third party tracking for advertising purposes.

This level of granularity is not appropriate to all enterprises or all contexts. For example, many companies use different providers to help operate their businesses. These could be payment processors, delivery companies, or a website host or cloud provider. It would not make sense for consumers to have a choice over the use of these providers since it would interfere in the company's basic business operations, as well as the ability to perform services the consumer requested.

Personal Information Rights

IA members also support user rights to access, deletion, correction, and portability. These rights provide users control over their personal information by allowing them to take action after the information has been collected. IA included these rights in the IA Privacy Principles:

- *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. 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.

IA members have been leaders in implementing tools to empower individuals to have control over the data they share. Not only are individuals given the controls

described above, but they are often able to access the personal information they have shared with an Internet company in real-time, without submitting a special request. They may be able to download that data directly in a commonly-used file type with a few simple mouse clicks, or by submitting an online request to the provider. Individuals may be able to directly edit their customer records and even remove records about their past use of the service—such as messages and photos, searches performed, products purchased, or streaming content viewed. This type of access to data that facilitates the exercise of user rights, existed in the Internet industry years before GDPR and the California Consumer Privacy Act (CCPA), and should be expanded to all entities that control personal information.

Elements Of Comprehensive Privacy Legislation

IA believes that Federal legislation should create individual personal information rights and rules for entities that process personal information on a nationwide basis, covering all unregulated sectors or harmonizing with sectoral regulation, and applying equally to online and offline environments—particularly for companies that don't have direct relationships with consumers or where people didn't sign up for a company's product or service. For this legislation to be successful in building trust in the entities that process personal information, without adversely impacting innovation, the legislation will have to be flexible, capable of evolving with changes in technology, and focused on privacy outcomes rather than prescribing how to achieve them.

For a Federal standard to address privacy across sectors, organizations of different scale, and different business models, it will need to be flexible enough to adapt to a range of entities processing personal information in varying contexts and for different purposes. A Federal standard should not introduce barriers to entry for small and new businesses. As organizations grow, the expectations regarding the measures they implement to protect personal information can also grow. The FTC has recognized the importance of adjusting security and data protection compliance obligations to match the size and complexity of organizations, and a Federal legislative framework that mirrors this approach will benefit consumers and businesses alike.

A Federal standard must also be written so that it can adapt to currently unknown, but nevertheless inevitable changes in the technology used to collect, store, use, and transmit data. To that end, it is better to build structures that focus on assessing and mitigating risk. Many of the services that have revolutionized our daily lives, such as home assistants, using our fingerprints or cameras to unlock devices, real-time traffic information, and GPS trackers for fitness would have seemed scary and full of risk 20 years ago. These products and services only exist because government policies have been largely successful in preserving individual rights while allowing technological innovation, including in the field of encryption, to flourish. We should not interfere with the next generation of advances.

To withstand the passage of time, a law also needs to be careful not to be overly prescriptive about the processes, technologies, or requirements for meeting a privacy objective. We do not have to look hard to find examples of data-focused laws that embraced the prevalent technologies of their time, but have struggled to keep pace with innovation. The Electronic Communications Privacy Act ("ECPA") is a good example. Congress was wise to recognize so early that electronic communications would revolutionize both business and personal interactions, but notwithstanding that foresight, the legislative language expressly applies to specific categories of service providers that existed at the time, and the types of data they collected, stored, and used. As technology and services evolved, ECPA fell behind. Before cloud-based e-mail became a prevalent mode of communication, many viewed e-mails kept for more than 6 months as inconsequential information that did not require a search warrant. Today, e-mail is often used as a personal lock box, and government may rely on lesser privacy standards to access electronic copies of personal information, even though a search warrant would be required to access that same information in the physical world. Federal data privacy legislation should be drafted to focus on desired outcomes and should not be specific to technology, to allow organizations to determine the best way to achieve that outcome in their operating environment, including other privacy laws.

Flexibility in Federal privacy law is also important to allow harmonization with global privacy laws that impact the operations of many U.S.-based organizations. The U.S. should adopt rules that make sense for the American public, while also enabling the U.S. to maintain important mechanisms that facilitate cross-border data flows and add to the developing global consensus around the core building blocks of personal privacy laws.

A Risk-Based Approach

IA believes that we have the opportunity to develop a strong and uniquely American approach to privacy that focuses on addressing the risk of harm to the individual, and that by focusing on identified risks we can deliver more meaningful privacy protections without imposing unnecessary burdens and restraints on innovation. IA's Privacy Principles explain:

- *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.

An American approach to privacy should consider the context of the interaction between the individual and the entity collecting the data. For example, you expect a car rental company to be able to track the location of a rented vehicle that doesn't get returned. You don't expect the car rental company to track your real time location and sell that data to the highest bidder. By focusing our efforts on addressing unexpected uses of data that pose risks to individuals, we can protect privacy without inundating people with information about things—like notices about cookies—if they are consistent with consumers' reasonable expectations. We should focus on providing people with the most important information they need to make informed choices about their privacy.

We are at an inflection point where it is critical that privacy and security considerations be integrated into risk management frameworks for organizations that process personal information, and into the product development process for organizations that build data-driven products. Efforts like NIST's Privacy Framework may provide important tools that organizations across all sectors and of all sizes can use to assess privacy risks on an ongoing basis. It can also educate organizations on potential options for risk mitigation. Federal legislation can support this cultural shift by incentivizing the use of tools like the NIST frameworks on privacy and security, security certifications, privacy certifications, sector specific tools like codes of conduct, and FTC education efforts designed to raise awareness of individuals.

Responsible Data Security Practices

User trust is fundamental to the success of Internet companies, and responsible data practices are critical for earning and maintaining user trust. Any company processing personal data should do so responsibly, acting as good data stewards. While less visible to individuals, an organization's internal controls can be as important, if not more important, to protecting the privacy of personal information as external facing information and mechanisms. These controls do not have to be formal or elaborate to be effective, but they must be focused on identifying and mitigating risk. They should consider the entire lifecycle of personal information within the organization and ensure the information is properly collected, used, shared, and secured.

Reasonable security measures are critical to maintaining the privacy of personal information, and IA believes that no comprehensive privacy law will be complete without a requirement that covered entities adopt appropriate technical and organizational measures to protect the confidentiality, integrity, and availability of personal information. The best privacy policy and user controls mean little if an individual's personal information can be easily compromised by a bad actor.

IA also believes that security breach notification is an important element of comprehensive legislation to protect personal information. Breach notification allows individuals to take action to protect themselves from the risks that result from having personal information acquired by unauthorized parties. This could include monitoring for identity theft, credit freezes, and password changes. IA has long⁶ supported Federal breach notification laws and has included breach notification as a key element for Federal privacy legislation in the IA Privacy Principles. All 50 states and many U.S. territories now have breach notification requirements. A Federal standard for breach notification would ensure that residents throughout the United States benefit from the same level of protections and receive consistent access to key information when their personal information is compromised.

⁶<https://internetassociation.org/031815datasecurity/>

Security requirements and security breach notifications are important elements of privacy legislation, but IA is also sensitive to the risk that the more elements added to legislation, the more complex it is for it to become law. There are existing breach notification requirements covering most of the United States, thus the level of urgency for a Federal breach law is not as high as it is for an economy-wide Federal privacy law.

Meaningful Enforcement

Companies that engage in unfair and deceptive trade practices that harm consumers should be held accountable. The FTC is the appropriate agency to enforce consumer-focused data privacy and security laws. The FTC has demonstrated expertise in privacy and security and a commitment to engaging in enforcement activity designed to improve the level of protections that consumers receive across entire sectors, not just from a single company.

The goal to have a Federal standard for personal information protection will require a strong lead regulator. This is not to say that the FTC must be the only regulator who can enforce a Federal privacy law, but that it should retain oversight on enforcement activities to ensure consistent application of the law.

A Federal privacy law that covers all entities that process personal information that are currently unregulated will clarify and expand the FTC's enforcement authority and responsibility. IA member companies strongly support providing the FTC with the resources needed to execute those responsibilities. IA member companies also believe the FTC should continue its mission of educating individuals on their rights and protections under the law, and this effort should be encouraged and appropriately resourced. The FTC also educates organizations on their obligations and best practices through efforts such as the Cybersecurity for Small Business campaign. These types of campaigns and guidance documents provide vital resources for smaller businesses that need additional clarity on how legal obligations apply to their specific organizations.

An enforcement regime should foster a culture of accountability and responsibility and will depend on the rest of the bill.

Conclusion

Internet Association and our member companies stand ready to work with this Committee and all other interested parties on an American approach to protecting people's privacy that allows for continued U.S. leadership in technology. The time is now for a national privacy law that provides consumers in every state both on and offline meaningful control over data in all sectors of the economy. Our goal is to see bipartisan legislation signed by the president this year.

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-dependent 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.⁷ 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.⁸ 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.

- *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 analyzed 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.

⁷These 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-SPAM 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.

⁸These 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.

- *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.

The CHAIRMAN. Thank you, Mr. Beckerman. And let me commend both of our first two witnesses on impeccable timing on the 5-minute rule. Mr. Dodge, you are now recognized.

STATEMENT OF BRIAN DODGE, CHIEF OPERATING OFFICER, RETAIL INDUSTRY LEADERS ASSOCIATION

Mr. DODGE. Thank you, sir. Chairman Wicker, Ranking Member Cantwell, members of the Committee, my name is Brian Dodge and

I am the Chief Operating Officer for the Retail Industry Leaders Association. Thank you for the opportunity to testify today about consumer privacy, Federal data privacy legislation and the care that retailers take in approaching privacy.

Despite the rapid transformation of the retail ecosystem, our members' core business remains straightforward—to sell products and services to customers. To do so, retailers have always sought to know their customers well in order to serve them better. While methods and technologies may have changed, leading retailers are guided by this simple purpose, and it is why we care so deeply about the conversation we are engaging in today. Retailers support Congress's leadership in finding a sensible path to set clear privacy expectations for all Americans through Federal data privacy legislation. The convergence of retail and technology has transformed the retail industry and greatly empowered consumers.

Today, while consumers can still reach retailers in physical stores, they can now connect through websites, apps, and through search and social media platforms. Competition in retail is now a click or voice command away. This competitive environment means that retailers must maintain and deepen the trust in customer relationships. Robust competition ensures a daily referendum in the state of a retailer's relationship with their customers. Unlike some tech or telecom companies who tend to dominate their sectors, if a customer loses trust in one retailer, they can easily shop with another. These critical customer relationships shape retailers' approach to meeting consumer privacy expectations.

As retailers look to personalize the shopping experience, they rely on data that customers provide and data that they collect when customers interact with their brands. Retailers who better know their customers can offer products that customers want. Whether it is stocking Ole Miss shirts and blankets in football season, or the right Gonzaga gear in basketball season, personal information helps retailers decide how much merchandise to buy, where it needs to be, and when. Customer data not only helps retailers make important decisions throughout their supply chains, but it also produces dividends for customers. For many retailers, loyalty programs are an essential component of their business model and one that provides mutual benefit. Customer data also enables services customers demand. For busy families, the ability to pick up groceries with the convenience of drive-through is a game changer. Customer data also enables beneficial curated experiences. Offerings like baby registries enable new parents to discover curated products that they might not know they will need.

Personal information fuels other services leading retailers provide to benefit communities, such as flu trackers. These flu trackers are compiled using retail prescription data across thousands of stores.

Leading retailers recognize the unique moment we are in today. There is bipartisan opportunity to create a uniquely American privacy framework. RILA believes that a Federal privacy framework should be designed to protect customers and provide clear rules of the road for individuals, businesses, and for the Government. Retailers are prepared to accept the responsibility of new privacy re-

quirements to create a national framework that inspires consumer confidence.

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

In closing, retailers are committed to working with Congress to develop a strong Federal privacy standard based on these elements to protect consumers without stifling innovation, investment, and competition.

Thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Dodge follows:]

PREPARED STATEMENT OF BRIAN A. DODGE, CHIEF OPERATING OFFICER,
RETAIL INDUSTRY LEADERS ASSOCIATION

Chairman Wicker, Ranking Member Cantwell and Members of the Committee, my name is Brian Dodge and I am the Chief Operating Officer of the Retail Industry Leaders Association (RILA). Thank you for the opportunity to testify today about consumer privacy, Federal data privacy legislation and the care retailers take in approaching privacy. Despite the rapid transformation of the retail ecosystem over the past two decades, our members' core business remains straight forward—to sell products and services to customers. To do so, retailers have always sought to know their customers well in order to better serve them—from the friendly chat at the market stall to recommending new products at the general store—retailers have always tried to learn more about their customers' needs and preferences in order to improve their shopping experience. While methods and technologies may have changed, leading retailers are guided by this simple purpose, to better serve customers. It is why we care so deeply about the national conversation on privacy we are engaging in today. Retailers support Congress' leadership in finding a sensible path to set clear privacy expectations for all Americans through Federal data privacy legislation.

RILA is the U.S. trade association for leading retailers. We convene decision-makers, advocate for the industry, and promote operational excellence and innovation. Our aim is to elevate a dynamic industry by transforming the environment in which retailers operate. RILA members include more than 200 retailers, product manufacturers, and service suppliers, which together account for more than \$1.5 trillion in annual sales, millions of American jobs, and more than 100,000 stores, manufacturing facilities, and distribution centers domestically and abroad.

Retail Today

U.S. and global consumers are driving change in retail like never before. Ubiquitous Internet access coupled with changing consumer values, preferences, and lifestyles, have led to significant disruption in the industry. This digital revolution continues to transform the way customers interact with retailers and buy products. And the pace and depth of these changes are both unprecedented and accelerating. Retailers are adapting to this new consumer landscape through the pursuit of transformative innovation. The convergence of retail and technology (RTech) means that the retail business model has fundamentally changed, resulting in a business imperative to meet the desires of highly empowered consumers who have many choices

for how and where to shop. To thrive in this era, retailers must maintain and deepen trust in customer relationships.

Customers can still reach retailers in physical stores and can now connect directly through digital mediums like websites and apps and indirectly through search and other social media platforms. Competition in retail is now a click or voice command away which means that retailers operate within the most competitive industry in the world. This competitive environment has empowered consumers, which means retailers must focus on more than the transaction. They must focus on building and maintaining long-term relationships with customers through positive interactions and experiences. Customers' high expectations for how retailers safeguard their data to power these interactions and experiences is equal to their expectations regarding the quality of the products they buy. Failure to meet their expectations erodes the trust that is essential to maintaining a mutually beneficial customer-retailer relationship. Robust competition in retail ensures a daily referendum on the state of retailers' relationship with their customers. Unlike some tech or telecom companies whose services or platforms tend to dominate their sectors, if a customer loses trust in one retailer, they can easily shop with another. These customer relationships grounded in trust shape how retailers approach meeting customer privacy expectations and needs.

Retailers Use Customer Data to Benefit Customers

As retailers look to personalize the experience for their customers, they rely on data that customers provide, and data that they collect when customers interact with their brands, to help those customers find the products and services they want at the time, place, and manner of their choosing. Leading retailers seek to use customers' data to better serve customers. Everyone in this room shops online, mobile, and in-store. You can all appreciate when technology or good service makes your life easier and the shopping experience better. It is within this context that leading retailers collect and use personal information and customer data.

Retailers who better know their customers can offer products that customers want. Customer data is what tells a retailer to stock your favorite brands, in the right varieties, at the right time, and in the right place. Whether it is stocking Ole Miss shirts and blankets in football season or the right Gonzaga gear in basketball season, personal information helps retailers decide how much merchandise to buy, where it needs to be and when. Data fuels retailers' ability to ensure that the small home improvement contractor can order supplies to be delivered to the appropriate jobsite and the crafter can get their holiday supplies. Knowing what customers purchase also helps retailers stock up stores before natural disaster events with the products customers need most.

Customer data not only helps retailers make important decisions throughout their supply chains, but it also produces dividends for consumers. For many retailers, loyalty programs are an essential component of their business model, and one that provides mutual benefit. Loyal customers receive discounts and curated services and products, and retailers gain valuable insight into customer needs and preferences. Loyalty programs enable retailers to offer teachers and parents key discounts or other special offers on classroom supplies at back to school time. These discount programs often help retailers give back to the communities they serve.

Customer data also enables the services customers demand. Leading retailers are now offering the ability to order online and pick up at the store without the customer ever leaving their car. Data tells retailers how many employees need to be assigned to provide that service, identifies peak times, and specifies locations. For the dad or mom of little kids, picking up diapers or groceries with the convenience of drive-through is a game changer. Many leading retailers now offer delivery services, often in as short as two hours. Consumer opt-ins sharing geolocation or personal information ensures delivery of products to any desired location.

Personal information also enables beneficial curated experiences. When consumers interact with retailers online or via mobile app, it is personal information that allows the customer to see products and deals that are more relevant to their needs. It also allows retailers to understand the context of their relationship with each unique consumer, and to prompt individual customers with offers that are tailored to their needs and preferences. The Sunday circular once arrived on your doorstep and gave everybody one list of what was on sale within a given week in a store. Data allows leading retailers to leverage technology and advanced supply chains to target individual consumers with offerings tailored to their needs and lifestyle. Offerings like baby registries enable new parents to discover curated products based on their preferences that a new parent might not know they will need.

Personal information fuels other services that leading retailers provide to benefit communities such as flu trackers. Developed as a timely, local resource, consumers,

health officials and the media now use it to track flu activity in their community. These flu trackers are compiled using retail prescription data for antiviral medications used to treat influenza across thousands of stores. In addition to helping the public, retailers use this data to determine which communities should get more flu vaccines in stock, when there is a vaccine shortage, and where to direct stock of medications to treat the flu to ensure that enough medication is available when needed.

Retail data uses are clear and within the established context of a customer relationship. Customers are just that, customers—they are not users or products. This context differentiates retail from other industries who collect and use data in ways that are not well understood, anticipated, or desired. Retailers interact directly with customers and the collection and use of personal information is to better meet customer needs.

Retail Privacy Approach

Leading retailers embrace the careful stewardship of customer data not only because maintaining customer trust is a core business imperative, but because it is the right thing to do for customers. In designing data management systems, retailers think about the entire data lifecycle management process to determine how to collect, use, share, and protect personal information.

Retailers carefully consider a variety of elements to determine the necessity of data collection as well as the appropriate scope of collection. Some factors weighed by retailers in determining whether to collect data include customer benefits, business purpose of collection, customer insights available from the data, transaction friction, sensitivity and volume of data, and parts of the business that need the data. Retailers frequently evaluate whether a business need can be accomplished by some other means.

After retailers determine whether to collect consumer data, they also continue to reevaluate how that data is being used and stored and with whom it is shared. Leading retailers have invested heavily to protect their customers' data. Keeping personal information private begins with security. Finally, retailers determine the retention period for data to ensure that it is appropriately maintained, according to applicable law, and disposed of properly.

Retail Privacy Public Policy: A Pragmatic Approach

Leading retailers recognize this unique moment. The revelations of Cambridge Analytica coupled with legislative developments in Europe and California have fundamentally reoriented the national conversation on privacy. In today's climate, Democrats and Republicans may not agree on much, but they certainly agree on the importance of a new approach to privacy. Both the Obama¹ and Trump² Administrations have recognized the need to address privacy. There is a bipartisan opportunity to create a uniquely American privacy framework that embraces the dynamism of American ingenuity with the fairmindedness of making sure everyone gets a square deal.

A new privacy framework will require choices and artful balancing of interests. RILA believes that a Federal privacy framework should be designed to protect consumers and provide clear rules of the road for individuals, businesses, and the government. Retailers are prepared to accept the responsibility of new privacy requirements to create a national framework that applies to all parts of the data ecosystem and inspires consumer confidence.

Retail Privacy Public Policy: Elements

RILA believes there are six critical elements to a pragmatic and workable approach to privacy at scale.

1. *Consumer Control, Access, Correction, and Deletion Rights.* Leading retailers believe in respecting customers' wishes by providing reasonable control over their personal information. But, too often this debate descends into the binary options of mandatory consent for every use on the one hand and no consent for any use on the other. Retailers support providing control, access, correction, and deletion rights including allowing consumers to limit sharing data with

¹THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf> (last visited Feb 2019).

²NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, NTIA SEEKS COMMENT ON NEW APPROACH TO CONSUMER DATA PRIVACY, (2018), <https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy> (last visited Feb 2019).

third-parties like advertisers and restrictions on targeted advertising. Retailers believe that which controls to offer, when to offer them, and how they are offered should depend on context. For example, a transaction that includes delivery necessarily includes the transmission of a customer's address to the third-party delivery service. The context of this transaction should not require consent because transferring address information is necessary to meet the customer's desire for delivery. Context may also include a variety of legal, technical, financial, and security requirements that must be correctly weighed. For example, a retailer may need to retain consumer information when it is needed to secure a transaction, prevent fraud, or comply with the law. In addition, retailers believe that policymakers should carefully evaluate the implications of multichannel collection environments by recognizing that all collection is not electronic through easily consolidated data systems, but may include a variety of interactions such as one to one connections through store associates and service professionals. A privacy approach that evaluates data use in context better addresses the business models and uses of data in the marketplace today rather than relying on foundational consent models alone.

One area where retailers believe further scrutiny by policymakers is required involves data portability. This is an important concept which can, for example, enhance competition in the social media space. However, in other industries porting certain user generated data may ultimately create anticompetitive outcomes. To avoid these unintended consequences, retailers believe that protecting proprietary business methods requires limiting portable data to content generated and submitted by the user, which would exclude data such as inferences drawn by the organization about the user or other data generated by the organization.

2. *National Privacy Framework.* Leading retailers believe a sound privacy policy framework must be national in scope to better protect customers and reduce state-level burdens on interstate commerce. Purchases no longer occur in one place. Consumers may order a product online, that comes from a store or distribution center in another state. Despite these jurisdictions, it is critical that consumers have the same set of rules, safeguards, and protections across the United States that are clear and empower them to make choices and trust that their choices are adhered to, no matter the state jurisdiction. Strong Federal preemption is also necessary to prevent a balkanized regulatory landscape and bring uniformity and rationality to myriad potential approaches. We believe a national framework will better protect American innovation and allow companies to implement privacy by design, creating clear and predictable consumer outcomes to meet their expectations.
3. *Accountability for All Ecosystem Parties.* Leading retailers believe that every sector within the data ecosystem should have a responsibility to consumers. As Cambridge Analytica and Equifax have amply shown, third-parties and service providers who are often unknown to consumers must have the same responsibilities as consumer-facing companies. While contracts are certainly necessary, they should be bolstered by enshrining the responsibilities of all parties to be diligent stewards of consumer data into law.
4. *Risk-based Practical Scope.* Leading retailers believe in a risk-based approach to privacy. The core definition of sensitive personal information should be clearly linked to areas where there is a real risk of tangible harm. Creating a scope that allows companies to draw real boundaries around truly sensitive personal information while enabling non-sensitive data to be used to benefit customers is vital to having a functioning privacy policy framework. Critical to this risk-based approach is a precise and targeted definition of personal information. Overly broad definitions containing data that is publicly available, household level, de-identified, pseudonymous, harmless, or employee data should not be included in such a definition. In addition, data that is not reasonably capable of being associated with an individual should also be excluded. Unrealistic and broad mandates that are untethered to the realities of operating at scale or enhancing privacy should find no home in a Federal privacy law.
5. *Incentives for Good Faith Actors.* Retailers support creating incentives for good faith actors to go beyond baseline privacy requirements. For example, policymakers could create legal safe harbors for good faith actors who implement additional privacy enhancements beyond baseline privacy. Retailers believe one challenge to all potential frameworks is the volume, velocity, and complexity of data processing. Retailers believe providing such incentives will not only encourage companies to embrace innovative privacy practices and technologies,

but it may also serve to find new ways to eliminate impediments to enhanced consumer privacy. Incentives will encourage more services and products that are inherently designed to protect consumer privacy and business interests, and adapt as new privacy challenges emerge over time.

6. *Strong and Fair Enforcement.* Retailers support fair, consistent, and equitable enforcement of privacy laws. Retailers agree that the Federal Trade Commission is the appropriate enforcement agency along with state attorneys general, and that enforcement of privacy laws should be consistently applied based on cases of actual harm. Retailers recognize that beyond enhanced authority, the FTC will require additional resources to robustly enforce a Federal privacy law. Retailers strongly believe that enforcement through a single Federal expert agency and state attorneys general will create the correct balance between strong consumer privacy and harmful inconsistent enforcement that would occur if alternative mechanisms like private rights of action become widespread.

Retailers are Committed to Protecting Customer Data and Enhancing Consumer Trust

Retailers are encouraged by the Committee's bipartisan commitment to developing a Federal privacy standard to protect consumers without stifling innovation, investment, or competition. We are also encouraged that other policymakers, including the Department of Commerce's National Telecommunication and Information Administration and National Institute of Standards and Technology, are working to define an Administration approach and to create a risk-based privacy framework. With both Houses of Congress and the Administration's support, retailers believe a Federal privacy bill can become law.

Ultimately, leading retailers take a pragmatic approach to privacy that is grounded in the realities of operating global businesses that interact with millions of consumers in both the digital and physical world every day. Retailers' primary objective is to please customers. Consequently, the industry's guiding principle on consumer privacy is that data should be used responsibly to benefit customers. We encourage policymakers to be guided by that principle and to consider the practical impact a privacy framework will have on consumers. Retailers support this important effort and stand ready to work with policymakers and all stakeholders to continue to advance innovation and consumer privacy.

Mr. CHAIRMAN. Thank you, Mr. Dodge. And thank—the ranking member and I want to thank you for the references to Ole Miss and Gonzaga. And also, if you just wanted to do one reference that would have touched both of us that would have been Mississippi and Gardner Minshew who made his way to Washington State University and was an outstanding quarterback. Just getting that little plug in there.

[Laughter.]

Mr. CHAIRMAN. Ms. Espinel, we are glad to have you.

STATEMENT OF VICTORIA ESPINEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BSA | THE SOFTWARE ALLIANCE

Ms. ESPINEL. Thank you. Good morning, Chairman Wicker, Ranking Member Cantwell, and members of the Committee.

My name is Victoria Espinel and I am the President and CEO of BSA | The Software Alliance. I commend the Committee for holding this hearing on the important topic of a Federal data privacy framework, and I thank you for the opportunity to testify on behalf of BSA. We are here today because the American people's trust has been broken. Every morning, people wake up to a news report about their location being sold without their knowledge. When they go online, their movements around the web are tracked, allowing companies to profile them. Companies that people have never heard of, often know more about them than they know about themselves. And companies buy and sell that information to the highest

bidder. Sometimes the information is used for a legitimate purpose, but sometimes it is not. And this is unacceptable.

BSA is the global advocate for the software industry. BSA members have business models that promote, not undermine, privacy and security. Our businesses are not dependent on selling ads. There are different business models and different approaches to consumer data. There are different incentives when a company's business model is primarily the monetization of personal information. The driving force behind the success of our companies is the sale of innovative products and services, such as cloud computing, design and engineering, cyber security protection. Our customers pay for these products and services. We are partners with businesses of all sizes across every industry in the U.S. economy, helping them grow and thrive. But we know that we are not the only actors in the ecosystem, and we agree that it is time to clean it up. We want to ensure that companies use data in a way that empowers not exploits.

We call on Congress to pass strong, comprehensive privacy legislation based on three pillars, rights, obligations, and enforcement. First, legislation should give consumers the right to know and the right to control what happens to their personal information. Second, legislation should require strong obligations for companies to safeguard data and prevent its misuse. And third, legislation should provide strong, consistent enforcement. Let me begin with consumer rights.

First, consumers should have the right to know the categories of information an organization collects, how that information is used, and how it is shared. Second, consumers should be able to use that knowledge to exercise real control over their personal information. To say no to data being used in ways that they do not want. Certain data, for example, health data or financial data or information about a particular health condition a person might have, is particularly sensitive and companies using that data should first obtain explicit consent. Third, people should be able to access, correct, delete, and obtain a copy of their data. There may be important limits on these rights. For instance, to protect network security and free speech, but those limitations should be the exception.

The second pillar is strong obligations for companies. Consumer rights should be reinforced by obligations on companies that handle data responsibly. Companies that handle personal data should have mechanisms to ensure safeguards against privacy risks, including security breaches and inappropriate use of consumers' data. Congress should also ensure that a Federal privacy law provide clarity about the responsibilities of companies that play different roles in the complex data ecosystem.

All companies should have strong obligations, but those obligations should fit the kind of business that they are in and distinguish between controller and processor. The third pillar is enforcement. A strong Federal law also needs strong enforcement. The FTC should continue to be the primary Federal enforcer, but it needs new tools and the resources necessary to carry out its mission effectively. The FTC should have new authority to issue fines to hold companies accountable. Today, the FTC cannot issue a fine the first time a company violates Section 5, no matter how egre-

gious. That is wrong and it should be fixed. And we believe that State Attorneys General should be able to enforce a strong, comprehensive Federal privacy law on behalf of the residents in their States.

In closing, let me emphasize, a Federal law does not and should not mean a weak law. A strong Federal law should replace State laws without undermining privacy protection. States such as California have been leaders on this issue, passing laws aimed at enhancing privacy protection. The objective of a consistent national standard is not to weaken privacy protections provided by California or other State laws. Rather, our aim is to strengthen privacy protection by providing comprehensive, clear, and consistent protection for consumers across the country. The privacy framework I have outlined would help rebuild consumers' trust. Now is the time for Congress to act.

BSA stands ready to assist in the effort to accomplish this important goal, and I look forward to your questions.

[The prepared statement of Ms. Espinel follows:]

PREPARED STATEMENT OF VICTORIA ESPINEL, PRESIDENT AND CEO,
BSA | THE SOFTWARE ALLIANCE

Good morning Chairman Wicker, Ranking Member Cantwell, and members of the Committee. My name is Victoria Espinel. I am President and CEO of BSA | The Software Alliance.

BSA is the leading advocate for the global software industry in the United States and around the world.¹ Our members are at the forefront of developing cutting-edge, data-driven services that have a significant impact on U.S. job creation and the global economy. I commend the Committee for holding this hearing on the important topic of a Federal data privacy framework, and I thank you for the opportunity to testify on behalf of BSA.

This is the year to pass strong, consumer-centric privacy legislation, and BSA looks forward to working with this Committee to make it a reality. Privacy and security are core to establishing customer trust, which is necessary to realize the potential of the data economy to create jobs and improve lives.

We represent the enterprise perspective, meaning as you consider legislation, we urge you to remember that not all tech companies have the same business model. BSA companies don't rely on making money off of selling ads. They make money by selling products. They license software and sell services. They're partners with businesses of all sizes across every industry in the economy.

All of us care about privacy, and we particularly care about sensitive information. People may not mind if a photo of their dog is seen by the public. But people definitely care about outsiders tracking where they go, who they talk to, and which apps are sharing sensitive information with third parties without their knowledge. They care about their personal e-mails. They care about details of the business they've worked hard to build. They care about their private health and financial information. All of this information must be strongly protected.

That's why people choose our companies to protect their data. They entrust it to our companies, and BSA companies work very hard to keep that trust. That promise to protect your privacy is paramount. When you use Outlook to write an e-mail, Microsoft is not reading your e-mails to serve you targeted ads. When you use Salesforce to manage your relationships with customers, your customer lists stay secret.

BSA companies want Congress to pass a clear and comprehensive national law that gives consumers the right to know, the right to control, and the right to choose what happens to their personal information; imposes obligations on companies to safeguard consumers' data and prevent misuse; and provides strong, consistent en-

¹BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

forcement. Federal privacy legislation that includes these elements will protect consumer privacy interests, promote innovation, and promote global data flows.

Strengthening consumer privacy protections is a goal that BSA shares, and we urge you to pass strong data privacy legislation as soon as possible.

I. The Importance of Personal Data in the Digital Economy and the Widespread Benefits of Data-Driven Innovation

Over the last 20 years, consumers, businesses, and governments around the world have moved online to conduct business and access and share information. Services, including cloud computing, artificial intelligence (AI), and the Internet of Things, have transformed commerce, helping companies enter new markets and compete on a global scale. They have also delivered unprecedented efficiencies and considerable cost savings to every industry sector. As global leaders in the development of these data-driven products and services, BSA members prioritize the protection of consumers' personal data, and they understand that robust data protection is a key part of building consumer trust and promoting full participation in the digital economy.

The economic impact of software-and data-enabled innovation is enormous. In the United States, software contributes \$1.14 trillion to GDP and supports 10.5 million jobs, with an impact in each of the 50 states and across a range of industries. Software-enabled technologies increasingly rely on data and, in some cases, personal data, to perform their intended functions. Nearly ubiquitous network connectivity, growth in the number of connected devices, and improvements in algorithms and analytical techniques have led to dramatic, data-driven improvements in our ability to solve difficult societal challenges, bringing significant and widespread benefits and go far beyond business models that rely primarily on the monetization of consumers' personal data.

For example, AI technologies are providing myriad benefits to small and large organizations across a wide swath of industries, as well as consumers and society as a whole. To make AI work in practice, developers need access to data to build, evaluate, and maintain their systems. AI is helping organizations solve complex, rapidly changing, global problems, including:

- *Cybersecurity.* AI tools are revolutionizing how companies monitor network security by improving cyber threat detection, analyzing malicious behavior patterns, and detecting malware in real time. AI is also helping analysts parse through hundreds of thousands of security-related events per day to weed out false positives and identify threats that warrant further attention by network administrators. By automating responses to routine incidents and enabling security professionals to focus on truly significant threats, AI-enabled cyber tools help enterprises stay ahead of their malicious adversaries.
- *Fraud Detection.* AI is improving fraud detection by recognizing suspicious behavior and providing companies with real-time information that helps to identify and investigate different types of fraud, reducing the losses caused by malicious actors by billions of dollars. These tools also protect consumers from the risk of fraudulent charges and from the frustration associated with “false declines.”
- *Healthcare.* Software is helping medical networks coordinate care among hospitals, doctors, and health care facilities to reduce redundant care costs and improve health care quality. Additionally, AI is helping doctors predict patient risk for illnesses such as heart disease and create treatments.
- *Diversity and Inclusion.* AI is being used to promote inclusion. For instance, AI systems are at the heart of new devices and applications that can improve the lives of people with disabilities. AI is also helping people with vision-related impairments interpret and understand visual content, such as photos and their physical surroundings, opening new possibilities to navigate the world with increased independence and greater ability to engage in communities.

BSA companies use data in many other ways that help protect privacy and security. For example, services that help consumers and enterprises manage online identities to authenticate users not only provide strong security and protect privacy but also improve the user experience, making shortcuts that create vulnerabilities less attractive. Other BSA members provide privacy-enhancing technologies that use, for example, data masking, enabling companies to reduce the sensitivity of data they hold and mitigate privacy and security threats.

Cloud computing services provided by BSA members also improve security by implementing state-of-the-art, multilayered defenses and allowing customers to compartmentalize datasets, thereby preventing a breach in one location from impacting

the full dataset. BSA members know that the responsible deployment of these services requires dealing transparently with their customers. Users of these services entrust some of their most sensitive data—including personal data—with our members. As a result, privacy and security protections are fundamental parts of BSA members’ operations.

Finally, BSA members provide services that help other organizations grow and thrive. From human resources management to design and engineering, our members use data to develop and improve their products for customers all over the world. Indeed, BSA members also help their customers compete in a complex, global environment. Many BSA members provide services that power other businesses, including start-ups and small-and medium-sized enterprises. These services are designed to enable compliance across this broad range of customers, allowing them to enter markets that might otherwise be prohibitively expensive. Global interoperability in privacy laws, in turn, supports these efforts.

Maintaining global data flows is critically important to realizing many of these benefits, as well as developing and using cloud computing services to their maximum advantage. Global data flows enable companies of all sizes to reach customers and find suppliers across the world. Cross-border data flows also help fuel data analytics, which can deliver limitless socially and economically beneficial results in myriad contexts, ranging from digital commerce to natural disaster response. For example, hospitals and other healthcare organizations often need to transfer personal data across borders for use in clinical support software, which analyzes electronic health records, health insurance claims, and data sets to help caregivers improve the effectiveness of medical treatments and reduce overall health risks.

In short, BSA members provide data-driven services that are driving U.S. and global economic growth, provide substantial societal benefits, and enable the protection of the privacy and security of consumers’ personal data.

II. The Role of Federal Legislation

In addition to the experience that BSA members have with protecting personal data and complying with the EU General Data Protection Regulation (GDPR) and other privacy laws across the globe, BSA has a long history of engaging with industry, government, and other stakeholders to advance privacy protections.² For example, BSA has been an active participant in ongoing policy and framework development processes led by the Federal Trade Commission (FTC) and the Department of Commerce. BSA has also encouraged the U.S. government to discourage data localization measures and continue its efforts to facilitate cross-border data flows through frameworks such as the EU–U.S. Privacy Shield and the Asia-Pacific Economic Cooperation’s Cross-Border Privacy Rules system. These efforts have been critical to developing the digital economy as well as privacy best practices.

Now, as consumers face increased difficulty in navigating a more complex technological landscape, and as data practices among companies vary widely, BSA supports Federal privacy legislation to ensure that consumers receive appropriate privacy protections, organizations face clear obligations, and the United States maintains a strong position to protect global data flows.

More specifically, Federal privacy legislation should achieve three goals: give consumers the right to know, the right to control, and the right to choose what happens to their personal information; impose strong obligations on companies to safeguard consumers’ data and prevent misuse; and provide strong, consistent enforcement.

A. *Providing Strong Privacy Rights for Consumers: The Right to Know, the Right to Control, and the Right to Choose*

Transparency. Federal legislation should require organizations to provide users of their services with clear and accessible explanations of their practices for handling personal data. Providing consumers with information that enables them to understand how an organization processes personal data directly supports the aim of giving them more control over their personal data.

However, providing this information in a manner that is helpful to consumers can be challenging.³ Determining how best to provide information to consumers may depend, among other things, on the types of data at issue as well as the kind of services that an organization offers to consumers. Companies therefore need sufficient

²See generally BSA | The Software Alliance, Privacy Framework (released Sept. 12, 2018), https://www.bsa.org/~media/Files/Policy/BSA_2018_PrivacyFramework.pdf (“BSA Privacy Framework”).

³See, e.g., Notice and Request for Comments, Developing the Administration’s Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,601 (Sept. 26, 2018) (noting that “lengthy notices describing a company’s privacy program at a consumer’s initial point of interaction with a product or service” are part of the current “paradigm” of privacy notices).

flexibility to communicate information about their data practices in order to best inform consumers. Still, there are certain types of information that in most, if not all, circumstances are useful to provide to consumers and therefore are worth considering incorporating into Federal legislation as generally applicable requirements, including: (i) the categories of personal data that organizations collect; (ii) the type of third parties with whom they share data; and (iii) the description of processes the organization maintains to review, request changes to, request a copy of, or delete personal data.

Informed Choice. Consumers should be able to exercise appropriate control over their personal data. Although notice and choice alone may not address all privacy challenges, in appropriate settings, consumer choice still has an important role to play.

Organizations should provide consumers with sufficient information to make informed choices and, where practical and appropriate, the ability to opt out of the processing of personal data.

Organizations should consider the sensitivity of personal data at issue. Certain data, such as information about an individual's financial accounts or health condition, may be particularly sensitive. Requiring organizations to obtain affirmative express consent from consumers when collecting this sensitive information is appropriate under many circumstances.

Sensitivity-based obligations help to ensure that privacy protections comport with consumers' expectations, generally offering the strongest protections in settings that present the greatest risk of concrete harm to consumers. Personal data types that should be classified as sensitive are: precise geolocation data; unique, government-issued identifiers; biometric data; genetic data; financial account information; medical information; the contents of communications (with respect to an entity that is not an intended recipient of the communication); and personal data that relates to a consumer's racial or ethnic origin or sexual orientation.

Access, Correction, and Deletion. In light of the increasing challenges that consumers face in understanding the implications of choices and the growing range of circumstances in which implementing choice is infeasible, consumers should have other ways to improve their control over personal data. In particular, consumers should be able to request information about whether organizations have personal data relating to them as well as the nature of such data. In addition, consumers should be able to request a copy of the data, challenge the accuracy of that data, and, where relevant and appropriate, have the data corrected or deleted. With appropriate access to the personal data that organizations hold about them, consumers can make more informed decisions about whether and to what extent to use that organization's services. Organizations that determine the means and purposes of processing personal data should be primarily responsible for responding to these requests under Federal privacy legislation.

Federal legislation should also set certain limits on the ability of consumers to request a copy of, access, correct, or delete personal data. In particular, companies must have the flexibility to deny these requests when the burden or expense of fulfilling a request would be unreasonable or disproportionate to the risks to the consumer's privacy. In addition, organizations should have the ability to deny access, correction, or deletion requests in order to promote other important interests, including compliance with legal requirements; the protection of network security and confidential commercial information; conducting research; and avoiding the infringement of privacy, free speech, or other rights of other consumers.

B. Establishing Strong Obligations for Companies to Safeguard Consumer Data and Prevent Misuse

Although it is important for Federal legislation to give consumers better ways to make informed choices about personal data and exercise control over it, other measures may be necessary to ensure sufficient privacy protection. Organizations that handle personal data should have processes in place to ensure that their safeguards appropriately address privacy risks, including but not limited to the prevention of inappropriate uses of data, security breaches, and other incidents that may harm consumers' privacy. BSA therefore supports including security and accountability in Federal privacy legislation.

Security. Data security is integral to protecting personal data and privacy. Currently, however, companies must navigate a complex tangle of data security laws, rules, and standards—some of which are difficult to decipher and apply, while others are in conflict with one another. To address these issues, Federal privacy legislation should also establish a harmonized baseline data security standard.

A Federal data security standard should require organizations to employ reasonable and appropriate security measures designed to prevent unauthorized access,

destruction, use, modification, and disclosure of personal data based on the volume and sensitivity of the data, the size and complexity of the business, and the cost of available tools. A data security standard also should take into account the wide range of security risks that companies face, the rapidly changing nature of security threats, and the complexity of developing security standards. Accordingly, data security requirements must be flexible, and they should be consistent with internationally recognized standards that also are risk-based, technology-neutral, and outcome-focused.

Accountability. Accountability within organizations that handle personal information is also critical to effective data protection. The central objective in accountability is for organizations that process personal data to remain responsible for its protection, no matter where or by whom the data is processed. Policies and practices that govern how an organization as a whole handles personal data are essential to ensuring that the organization identifies relevant privacy risks and appropriately manages them. They also are essential to identify means that allow consumers effectively to exercise control over personal data. Specific elements that should underlie accountability include (i) designating persons to coordinate the implementation of these safeguards, including providing employee training and management; (ii) regularly monitoring and assessing such implementation; and (iii) where necessary, adjusting practices to address issues as they arise. Organizations should also employ governance systems that seek to ensure that personal data is used and shared in a manner that is compatible with stated purposes.

Each organization will have different lines of business and an array of other considerations that relate to how to structure and combine accountability practices. Therefore, providing flexibility in how organizations ensure their own accountability is important. More specifically, the use of any specific accountability mechanism should not be mandatory. Instead, privacy legislation should focus on the objectives of responsible data processing.

Notably, companies, including BSA members, are also using data in ways that both broaden inclusion, such as providing increased access to opportunities for people with learning disabilities or visual impairments, and helping other business customers understand better how the data and advanced technologies they are using lead to a range of outcomes, enabling other companies to be more transparent about the services they provide. In service of these objectives, companies maintain safeguards to mitigate the risk of bias or unlawful discrimination.

Controller/Processor Distinction. As Congress establishes strong obligations for organizations to implement, providing clarity about an organization's role and responsibilities in the complex, dynamic, data-driven economy can complement enforcement efforts by promoting business arrangements that reinforce those responsibilities. The distinction between controllers, which determine the purposes for which personal data is processed, and processors, which perform storage, processing, and other data operations on behalf of controllers, is key to allowing organizations that handle personal data to clearly define their responsibilities.

It is appropriate for Federal privacy legislation to impose different levels of responsibility on controllers and processors for achieving privacy outcomes. In particular, controllers, which determine the means and purposes of processing personal data, should have primary responsibility for satisfying legal privacy and security obligations. Controllers are the entities that, among other things, make decisions about consumers' data, including who it is shared with and how it is used.

On the other hand, processors, which handle data on behalf of the controller to implement the controller's objectives, should be responsible for securing the personal data they maintain and following the instructions pursuant to their agreements with relevant controllers. The processor/controller distinction provides organizations with a clear picture of their respective legal obligations, while still ensuring consumers are protected.

Importantly, adopting a distinction between controllers and processors and their levels of responsibility would promote interoperability among privacy frameworks and consistency in multinational, business-to-business contracts and other arrangements. The distinction is fundamental to privacy laws around the world, including the European Union's GDPR, and the many business relationships associated with global processing operations that have incorporated this distinction.

C. Provide Strong, Consistent Enforcement

Effective enforcement is important to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. The FTC has demonstrated that it is highly capable of overseeing and enforcing those commitments and obligations, as is evident from the more than 100 privacy and data security enforcement actions the agency has brought under Section

5 of the FTC Act.⁴ The FTC has also developed a deep understanding of the complexities of the digital economy. In addition, the FTC generally has observed the principle of bringing cases that remedy and deter harmful conduct, rather than punishing technical lapses. Given this strong record, the FTC should maintain its leadership role as the primary Federal enforcer of consumer privacy protections under Federal privacy legislation, and it should have the tools and resources necessary to carry out its mission effectively.

In addition, in order to provide consistent expectations for consumers and clear obligations for companies across the country, it would be appropriate for a strong Federal law to replace, but not undermine the protections in, state laws. We recognize that states, such as California, have been leaders on this issue, passing laws aimed at enhancing consumer privacy protections. Importantly, the aim of a consistent national standard is not to weaken privacy protections provided by California or other state laws. Rather, the aim is to strengthen those laws by providing comprehensive, clear, and consistent protections for consumers across the country. Moreover, we believe that state attorneys general should continue to have the ability to enforce a strong, comprehensive Federal privacy law. This will provide both better enforcement and a pathway for states to continue to promote and protect privacy.

III. The Path Forward

BSA members take their privacy commitments and obligations very seriously. At the same time, BSA members operate in a global environment that is increasingly complex in terms of technology, business and customer relationships, and regulation. A Federal privacy law that sets strong standards and brings consistency to existing protections would help protect privacy, promote innovation, and contribute to U.S. leadership on privacy issues in the global marketplace. BSA strongly supports these goals, and we look forward to working with the Committee to achieve them.

The CHAIRMAN. Thank you very, very much. Now, Mr. Randall Rothenberg with the Interactive Advertising Bureau.

STATEMENT OF RANDALL ROTHENBERG, CHIEF EXECUTIVE OFFICER, INTERACTIVE ADVERTISING BUREAU

Mr. ROTHENBERG. Chairman Wicker, Ranking Member Cantwell, members of the Committee, I am honored for the opportunity to testify today.

I am Randall Rothenberg, Chief Executive Officer of the Interactive Advertising Bureau. We represent more than 650 leading media and technology companies, consumer brands, and their hundreds of thousands of employees. The IAB develops technical standards and best practices to create efficient, effective, and safe digital marketing environments. We train industry professionals on these standards and practices. And we field critical research on the role of interactive marketing in growing brands, companies, and economies. Our experience shows there is a ready path forward to assure both the safety of consumers and continued growth in the consumer economy.

The Internet is the most powerful and empowering mode of communication and commerce ever invented. It is built on the exchange of data between individuals, browsers, and devices, and myriad server computers operated by hundreds of millions of businesses, educational institutions, governments, NGO's, and other individuals around the world. Advertising has served an essential role in the growth and sustainability of this digital ecosystem almost from the moment the first Internet browsers were released to the public in the 1990s. In the decade since, data-driven advertising has powered the growth of e-commerce, the digital news in-

⁴See FTC, *Privacy and Data Security Update 2*, 4 (2017).

dustry, digital entertainment, and a burgeoning consumer-brand revolution. But the source of the internet's innovation is also the source of its vulnerabilities.

The data exchanges that fuel new businesses and drive unprecedented cultural invention, can also be used to violate consumer security and privacy. The question before Congress is, how do we close off the sources of corruption without impeding the innovation. It is no easy task. The economy is in the midst of an enormous shift. Data increasingly is the core asset of every enterprise, replacing such a legacy asset as a company's manufacturing footprint or its access to raw materials. The greatest consumer brands of the 20th century are now being challenged by thousands of upstart brands in every category, which share one trait. Whether they make luggage, or beer, or cosmetics, or eyeglasses, or underwear, their success is premised on having individual relationships with millions of consumers. This is achieved only through the responsible use of data.

IAB strongly believes that legislative and regulatory mechanisms can be deployed in ways that will reinforce responsible use of data and enhance trust in the Internet ecosystem, while avoiding the unintended consequences that can result from ill-considered regulatory regimes. Notably, the erection of barriers to market entry and reinforced advantage for the largest incumbents. IAB has the ability to help guide Congress based on our experience building effective mechanisms to protect consumer privacy and security. These include the Digital Advertising Alliance's YourAdChoices and political ads programs, which provide consumers with transparency, control, and accountability in their digital advertising experience. Our industry is hardened by the Federal Government joining us in our long-standing effort to enhance privacy and security.

Our model is the partnership between Government and industry that created the modern concept of automotive safety in the 1960s. Yes, that partnership began as a shotgun wedding. Yes, the auto industry resisted at first, but an undeniable consumer right to be safe on the highways met well-researched solutions, which the Congress embedded in well-crafted laws that were supported by the States. The result has been millions of lives and billions of dollars saved. The analogy holds well here. Americans have a right to be secure on the information superhighway. Our goal should be to find the 5 or 10 practices and mechanisms, the seatbelts and airbags, of the Internet era that companies can implement, and consumers can easily adopt that will reinforce private, security, and trust. To begin, we believe it is vital that Government industry and consumer organizations establish a new paradigm for data privacy in the United States.

In developing this new paradigm, IAB cautions the Congress from relying on legal regime such as Europe's General Data Privacy Regulation or California's Consumer Privacy Act as models. These post stringent mechanical requirements on businesses but fall short in giving consumers real rights and choices. Opt-ins and opt-outs, I would suggest to you, are not the seatbelts and airbags of the information superhighway. IAB asks for Congress support in

developing this new paradigm that would follow four basic principles.

First, in contrast to many existing privacy regimes, a new law should impose clear prohibitions on a range of specifically identified, harmful, and unreasonable data collection and use practices. Second, a new paradigm should distinguish between data practices that pose a threat to consumers and those that do not. Third, it should incentivize strong and enforceable compliance programs, and thus universalize compliance by creating rigorous safe harbor processes in the law.

And finally, it should reduce consumer and business confusion by preempting the growing patchwork of State privacy laws. As with the rest of the witnesses, IAB asks for Congress's support in developing such a framework to enhance consumer privacy, and we want to work with you.

Thank you for the time today and I welcome your questions.

[The prepared statement of Mr. Rothenberg follows:]

PREPARED STATEMENT OF RANDALL ROTHENBERG, CHIEF EXECUTIVE OFFICER,
INTERACTIVE ADVERTISING BUREAU

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, I am honored for the opportunity to testify today. I am Randall Rothenberg, Chief Executive Officer of the Interactive Advertising Bureau. Founded in 1996 and headquartered in New York City, the IAB represents over 650 leading media and technology companies, and consumer brands that are responsible for selling, delivering, and optimizing digital marketing campaigns. Together, our members account for the vast majority of digital advertising in the United States. Working with our member companies, the IAB develops technical standards and best practices to create efficient, effective, and safe digital marketing environments, trains industry professionals on these standards and practices, and fields critical research on the role of interactive marketing in growing brands, companies, and economies. I have had the honor of testifying before Congress several times on the topic of privacy in digital media and advertising environments, and each time I offer up the same guidance and the same solutions. I am going to repeat myself once again, if with a bit more urgency, because I believe there is a ready path forward to assure both the safety of consumers and continued growth in the consumer economy.

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

Advertising has served an essential role in the growth and sustainability of the digital ecosystem almost from the moment the first Internet browsers were released to the public in the 1990s. In the decades since, data-driven advertising has powered the growth of e-commerce, the digital news industry, digital entertainment, and a burgeoning consumer-brand revolution by funding innovative tools and services for consumers and businesses to connect, communicate, and trade.

Data-driven advertising is not an Internet phenomenon; it has been a fundamental part of American business for well more than a century. But never in history has the open flow of data fueled such entrepreneurial and creative vigor, generating untold consumer benefit by enabling access to free content, services, and connectivity across once-insurmountable boundaries.

But these enormous benefits come at a price, and that is what we are here to address today. The source of the Internet's innovation is also the source of its vulnerabilities: an open, porous supply chain that allows any actor, no matter how creative *or* how corrupt, to plug and play—to invent a new business *or* poison a culture. The data exchanges that power new businesses and drive unprecedented cultural invention can also be used to violate consumers' security and privacy. The question before Congress is: How do we close off the sources of corruption and reduce the hazards without impeding the innovation?

This is no easy task. The economy is in the midst of an enormous shift; data increasingly is the core asset of every enterprise, replacing such legacy assets as a

company's manufacturing footprint or its access to raw materials. The greatest legacy consumer brands of the 20th Century are being challenged by thousands of up-start brands in every category, which share one trait: regardless of whether they make luggage, eyeglasses, underwear, or beer, their success is premised on having individual relationships with millions of consumers. This is achieved only through the responsible use of data. Customer relationships are improved across all industries by operationalizing consumer data. Such data is the essential driver of companies' growth, their ability to reach individuals at scale, and their creation of consumer value.

Central to companies' data-fueled growth is trust. As in any relationship, from love to commerce, trust underlies the willingness of parties to exchange information with each other, and thus their ability to create greater value for each other. The equation is simple: The economy depends on the Internet; the Internet runs on data; data requires trust. IAB strongly believes that legislative and regulatory mechanisms can be deployed in ways that will reinforce and enhance trust in the Internet ecosystem.

But in doing so, we must remain cognizant of the ways the economy—the pre-digital as well as the digital economy—have used data to foster growth, and strive not to disrupt the many legitimate means consumer data has been used to fuel innovation, economic growth, education, social organization, and culture. IAB, our members, and our sister trade associations stand ready to work with Congress to help craft a legislative and regulatory regime that protects consumers, while avoiding the unintended consequences that can result from ill-considered regulatory regimes, notably the erection of barriers to market entry, the erosion of competition, and reinforced advantage for the largest incumbents.

We recommend Congress start with a premise that for most of American history was self-evident, but today seems almost revolutionary: consumer data is a good thing. It is the raw material of such essential activities as epidemiology, journalism, marketing, business development, and every social science you can name. The United States recognized the centrality of consumer data to the growth of this Nation back in 1790, when we conducted the first census, and reinforced that centrality to the U.S. economy in 1902, when the Congress placed the Census Bureau under the auspices of the newly formed Department of Commerce and Labor. New data science and digital tools do not change the fact that data-based marketing is a reasonable and safe practice that has long been supported by the government. Fostering new private sector uses of data is a net good for consumers and the country that should not be curtailed through badly constructed controls.

Nor should we ignore the fact that something needs to be done by the Federal Government. As I appear before you today, the digital marketing and media ecosystem is at a crossroads. Recent events such as the Facebook-Cambridge Analytica scandal have placed a spotlight on companies' need to responsibly, safely, and transparently manage and use consumers' data, and make consumer privacy and security the foundational requirement for doing business in the modern economy. In response to those events, California, Washington, and other states are advancing new requirements and restrictions on businesses. These laws are well meaning and I support their intended goals. Nevertheless, elements of these proposals are reactive and risk stifling what should be understood as a uniquely American technological advantage. As a result, due to the emergence of conflicting state law regimes, consumer privacy has quickly become an area that needs Federal leadership and engagement.

Uniquely among today's speakers—and, I believe, any other witnesses you may call before you—the IAB and our trade association partners have the ability to provide Congress with a guide based on our experience building effective mechanisms to protect consumer privacy and security, such as the Digital Advertising Alliance's ("DAA") YourAdChoices and PoliticalAds programs that provide consumers with transparency, control, and accountability in their digital advertising experience,¹ and the Trustworthy Accountability Group ("TAG"), the organization that protects consumers and businesses alike from fraudulent digital advertising, malware, and ad-supported piracy.² While hundreds of companies have signed on to these programs, and even nonparticipants have faced enforcement actions, by force of law, Congress is best able to ensure the broadest level of compliance. Consequently, our industry is heartened by the federal government joining us in our longstanding effort to enhance consumer privacy and security. In fact, if Congress were to give our

¹ See www.youradchoices.com; www.aboutpoliticalads.org.

² See www.tagtoday.net.

programs the force of law tomorrow, building on our work and going further, many consumer privacy and security concerns would be mollified almost immediately.

Consequently, we believe our goals align with the Congress' decision to take a proactive position on data privacy, rather than the reactive approach that has been adopted by Europe and some states. We believe we can work together as partners in this effort with you to advance consumer privacy. Our model is the partnership between government and industry that created the modern concept of automotive safety in the 1960s. Yes, the partnership began as a shotgun wedding. Yes, the auto industry resisted at first. But an undeniable consumer right—to be safe on the highways—met well-researched solutions, which the Congress embedded in well-crafted laws that were supported by the states. The result has been millions of lives and billions of dollars saved. We believe the analogy holds well here. Americans have a right to be secure on the information superhighway. Well-researched solutions and well-crafted laws can assure their “digital wellness.” We should be thorough, practical, and collaborative. Our goal should be to find the three or five or ten practices and mechanisms—the seat belts and air bags of the Internet era—that companies can implement and consumers can easily adopt that will reinforce privacy, security, and trust.

To begin, we believe it is vital that government, industry, and consumer organizations establish a new paradigm for data privacy in the United States, based on strong principles and underpinned by mechanisms to achieve those principles. Together, based on our members' experience, we can achieve this new paradigm by developing a Federal privacy law that, instead of bombarding consumers with notices and choices, comprehensively provides clear, even-handed, consistent, and predictable rules of the road that consumers, businesses, and law enforcers can rely upon. Without a consistent, preemptive Federal privacy standard, the patchwork of state privacy laws will create consumer confusion, present significant challenges for businesses trying to comply with these laws, and ultimately fall short of consumers' expectations about their digital privacy. We ask the Congress to harmonize privacy protections across the country through preemptive legislation that provides meaningful protections for consumers while allowing digital innovation to continue apace.

In developing this new paradigm, IAB cautions the Congress from relying on legal regimes such as Europe's General Data Privacy Regulation (“GDPR”) or California's Consumer Privacy Act (“CCPA”) as models for how a privacy standard should function. While well-intentioned and important developments in bringing deserved attention to the issue of data privacy, these rigid frameworks impose significant burdens on consumers while failing to stop many practices that are truly harmful; they also fail to recognize the various ways in which digital advertising subsidizes the plentiful, varied, and rich digital content and services consumers use on a daily basis and have come to expect. Consumers enthusiastically embrace the ad-supported model *because of* the free content and services it enables. They are aware of and support the exchange of value in which data-driven advertising funds the free or reduced-cost services they receive. In fact, a Zogby survey commissioned by the DAA found that consumers assigned a value of nearly \$1,200 a year to common ad-supported services, like news, weather, video content, and social media. A large majority of surveyed consumers (85 percent) like the ad-supported model, and 75 percent said they would greatly decrease their engagement with the Internet were a different model to take its place under a miscalibrated legal regime.³

The economic contribution of the ad-supported economy is undeniable. IAB research from 2017, conducted with Harvard Business School Professor John Deighton, found the ad-supported Internet created 10.4 million jobs. Calculating against those figures, this ecosystem contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6 percent of U.S. gross domestic product.⁴ Congress should embrace a new paradigm for privacy that does not curtail these goods and services that consumers seek on the Internet.

Moreover, GDPR and CCPA appear likely to fail to achieve their stated goals. GDPR, for example, poses stringent, mechanical requirements on businesses but falls short in giving consumers real rights and choices—and does nothing to implement actual privacy and security mechanisms. Consent banners and pop-ups that were supposed to impose limits on companies have been notably ineffective at curbing irresponsible data practices or truly furthering consumer awareness and choice. Opt-ins and opt-outs, I would submit to you, are not the seat belts and air bags of the information superhighway.

The CCPA, for its part, could actually harm consumers by impeding their access to expected loyalty programs and subscription renewal messages; divulging their

³ See www.digitaladvertisingalliance.org/press-release/zogby-poll.

⁴ See www.iab.com/economicvalue.

personal information to unintended recipients due to the lack of clarity in the law; and allowing unregulated third parties to access personal information in the guise of facilitating consumer requests. In addition, the CCPA's unclear drafting has created a level of uncertainty that has some businesses questioning whether they will be forced to pull out of the California market altogether—something that already has happened in Europe.⁵ The United States should, therefore, learn from the lessons of the GDPR and CCPA by creating a new paradigm for privacy protection that offers clarity and flexibility, both of which are critical to effective privacy protection.

Consumers want to know their privacy is protected, but they cannot spend hours every day finding and reading privacy notices. Our goal should not be to place more burdens on consumers, but to make their privacy protections reflexive, if not automatic. To start, we are asking Congress to develop clear rules about what data practices should be prohibited and what data practices should be permitted. Just as when rules for food, pharmaceuticals, and automobile safety were developed, consumers should be able to look to Congress to create reasonable, responsible, and sensible rules of the road to protect their privacy.

To achieve this goal, IAB asks for Congress' support in developing a new paradigm that would follow these basic principles: First, in contrast to many existing privacy regimes, a new law should impose clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified in the law. Second, it should distinguish between data practices that pose a threat to consumers and those that do not, rather than taking a broad-brush approach to all data collection and use. Third, it should incentivize strong and enforceable compliance programs, and thus universalize compliance, by creating a rigorous "safe harbor" process in the law. And finally, it should reduce consumer and business confusion by preempting the growing patchwork of state privacy laws.

IAB asks for the Congress' support in developing such a framework to enhance consumer privacy. Thank you for time today. I welcome your questions.

The CHAIRMAN. And thank you, Mr. Rothenberg. Dr. Woodrow Hartzog. Dr. Hartzog, I understand you have a Mississippi connection?

Dr. HARTZOG. That is correct, Senator. I am from—born and raised in Mississippi.

The CHAIRMAN. And there was a TV personality named Woodie Assaf.

Dr. HARTZOG. That is correct. He was my grandfather.

The CHAIRMAN. Terrific. Good. Well, welcome.

**STATEMENT OF DR. WOODROW HARTZOG,
PROFESSOR OF LAW AND COMPUTER SCIENCE,
NORTHEASTERN UNIVERSITY SCHOOL OF LAW
AND KHOURY COLLEGE OF COMPUTER SCIENCE**

Dr. HARTZOG. Thank you. Chairman Wicker, Ranking Member Cantwell, and members of the Committee, thank you for inviting me before you to provide testimony.

My name is Woodrow Hartzog and I am a professor of Law and Computer Science at Northeastern University. My comments today will address what I have learned from my research on privacy law. Specifically, I will focus on one particular conclusion. Our current privacy regime asks too much of people and too little of those en-

⁵Following the implementation of the GDPR, some smaller U.S.-based companies and publishers chose to exit the European market instead of risk the fines related to potential GDPR violations. Hannah Kuchler, *Financial Times*, *U.S. small businesses drop EU customers over new data rule* (May 24, 2018) <https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-221e7146b04>; Jeff South, Nieman Lab, *More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect* (Aug 7, 2018) <http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/>. Additionally, some companies chose to charge European users more for access to content because of an inability to run effective and profitable advertising in that market. Lucia Moses, *Digiday*, *The Washington Post puts a price on data privacy in its GDPR response—and tests requirements* (May 30, 2018) <https://digiday.com/media/washington-post-puts-price-data-privacy-gdpr-response-tests-requirements/>.

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

The transparency and control contemplated by these frameworks is impossible in mediated environments. People can only click on the options that are provided to them and companies have incentive to leverage the design of their products to manipulate and wheedle people into oversharing. Internet users are gifted with a dizzying array of switches, delete buttons, and privacy settings. But these choices are too often an overwhelming obligation. People might remember to adjust their privacy settings on Facebook, but what about Instagram, Twitter, Google, Amazon, Netflix, Snapchat, Siri, Cortana, Fitbit, Candy Crush, their smart TV, their robot vacuum cleaner, their WIFI-connected car, and their child’s Hello Barbie. The problem with thinking about privacy as control is that if we are given our wish for more privacy, it means we are given so much control that we choke on it.

Meaningful data privacy reform must do more than merely strengthen commitments to transparency, consent, and control. Second helpings of “I agree” buttons and turgid, unreadable terms of use would not have prevented the Cambridge Analytica debacle or the epidemic of data breaches, nor will they prevent the problems of manipulation, discrimination, and oppressive surveillance that we face in the future of automation. We are only just beginning to see the human and societal cost of massive data processing and platform dominance.

In addition to core privacy-related harms associated with data collection and use, companies’ demand for personal information is negatively affecting our attention, how we spend our time, how we become informed citizens, and how we relate to each other. Phenomena like fake news, deepfakes, non-consensual pornography, online harassment, biased algorithms, oversharing on social media, addiction by design, and lives spent staring into our phones are at least partially attributable to or made worse by the personal data industrial complex. Marginalized communities, particular communities of color, shoulder a disproportionate risk of privacy abuses. We need broader frameworks for personal data not just because information is personal to us, but because the incentive to exploit it creeps into nearly every aspect of our technologically mediated lives.

My second recommendation is to adopt substantive and robust rules that protect people’s trust in companies and establish firm data boundaries that companies are not allowed to cross. Being trustworthy in the digital age means companies must be discrete with our data, honest about the risk of data practices, protective of our personal information, and above all, loyal to us, the data subjects. Our privacy framework should be built to encourage and ensure this kind of trustworthy conduct. Apart from rules, some

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

Finally, without structural support, resources, and a strong political mandate for enforcement, any data protection framework will be ineffective. Regulators need rulemaking provisions where necessary, robust civil penalty authority, and the ability to seek injunctions. Individuals should have private causes of action and rights as data subjects. In order to protect hard fought State privacy protections, Federal legislation should continue the tradition of acting as a floor not a ceiling for privacy rules. In conclusion, our rule should seek to protect people in groups instead of saddling them with the risk of online interaction. Only then can our digital ecosystem become sustainable.

[The prepared statement of Dr. Hartzog follows:]

PREPARED STATEMENT OF WOODROW HARTZOG, PROFESSOR OF LAW AND COMPUTER SCIENCE, NORTHEASTERN UNIVERSITY SCHOOL OF LAW & KHOURY COLLEGE OF COMPUTER SCIENCES

I. INTRODUCTION

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for inviting me to appear before you and provide testimony on this important issue. My name is Woodrow Hartzog and I am a Professor of Law and Computer Science at Northeastern University's School of Law and Khoury College of Computer Sciences. I am also a Non-resident Fellow at The Cordell Institute for Policy in Medicine & Law at Washington University, a Faculty Associate at the Berkman Klein Center for Internet & Society at Harvard University, and an Affiliate Scholar at the Center for Internet and Society at Stanford Law School. I have written extensively about privacy and data protection issues, including over thirty scholarly articles, essays, and book chapters. I have specifically addressed policy principles for data privacy frameworks in a number of academic articles.¹ My recent book explores possible privacy principles for the design of data technologies.² My comments today will address what I've learned from this research. I make these comments in my personal, academic capacity. I am not serving as an advocate for any particular organization.

The effort to identify policy principles for a Federal data privacy framework is necessary, urgent, and expansive. There are so many different issues to consider, including questions about preemption, enforcement mechanisms, regulatory structure, civil rights implications, law enforcement access, algorithmic accountability, and more. Policymakers should consider many different perspectives, including but not limited to people of color, people in the LGBTQ+ community, people with disabilities, women, and all communities that privacy law affects in different ways.

Because my time is limited, I focus my remarks on the topic I have spent most of my efforts researching over the past few years—the way our current privacy regime asks too much of people and too little of those entrusted with our data. I make two recommendations for the Committee.

First, I recommend that lawmakers should resist the traditional approach to data protection, which emphasizes transparency through notice to users and choice

¹Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUROPEAN DATA PROTECTION L. REV. 423 (2018); Neil Richards & Woodrow Hartzog, *The Pathologies of Consent*, 96 WASH. U. L. REV. (forthcoming 2019); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L. J. 1180 (2017); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Woodrow Hartzog & Neil Richards, *It's Time to Try Something Different on Internet Privacy*, THE WASHINGTON POST (Dec. 20, 2018). Parts of this testimony are adapted from some of this research.

²WOODROW HARTZOG, *PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* (2018).

through user consent. It passes the risk of online interaction from data collectors onto people under an illusion of protection. This “notice and choice” approach has failed.

Second, the best path forward is to move beyond traditional procedural regimes towards substantive and robust rules that garner people’s trust in entities and establish firm boundaries that companies cannot cross without consequences.

Meaningful data privacy reform must do more than merely strengthen commitments to concepts like transparency, consent, and control. Second helpings of “I agree” buttons and turgid, unreadable terms of use would not have prevented the Cambridge Analytica debacle, the epidemic of data breaches, or the harmful decisions and predictions made by wrongfully biased algorithms powered by personal data. Nor will they prevent the problems of manipulation, discrimination, and oppressive surveillance that we face in a future of automation. Lawmakers should instead create non-waivable robust and substantive duties and data mandates for companies.

II. NOTICE AND CHOICE IS IRREPARABLY BROKEN

The state of privacy is bad and getting worse. For years, the rate and scale of privacy failures has grown exponentially. The fragile wall that policymakers constructed forty years ago to mitigate the risks of databases is cracking. The time honored response has been to give users more control. From social media to biometric information, proposed solutions include some combination of “privacy self-management” concepts like control, informed consent, transparency, notice, and choice.³ These concepts are attractive because they seem empowering. They promise to put people in charge of what happens to their personal data. While notice and choice regimes enable the collection, use, and sharing of personal information, consumers are left people exposed and vulnerable. Meaningful progress requires more.

In basing policy principles for data protection on notice and choice, privacy frameworks are asking too much from a concept that works best when preserved, optimized, and deployed in remarkably limited doses. Our personal agency is required for self-management concepts to work and, after all, we are only human. Even under ideal circumstances, our consent is far too precious and finite to meaningfully scale.

A. Notice and Choice Models Are Not Scalable

The problem with notice and choice models is that they create incentives for companies to both hide the risks in their data practices through manipulative design, vague abstractions, and complex words as they shift risk by engineering a system meant to expedite the transfer of rights and relinquishment of protections.

But even the idealized, perfected transparency and control models contemplated by these frameworks is impossible to achieve in mediated environments. There are several reasons why.

First, the control companies promise people is an illusion. Entities inescapably engineer their technologies to produce particular results. People’s choices are constrained by the design of the tools they use. Companies decide the kind of boxes people get to check, the buttons that they press, switches they activate and deactivate, and other settings they get to fiddle with.

Data collectors have incentives to make users believe they have more control than they are actually given. People can only click on the options provided to them. Think of how parents create this illusion of control for their children, such as when I give my kids a choice between going to the park or the movies. They feel empowered and I avoid a trip to the pet store so I can stave off a conversation about a new puppy for one more week.

Data collectors also have incentives to leverage design to extract our consent. Companies create manipulative interfaces exploit our built-in tendencies to prefer shiny, colorful buttons and ignore dull, grey ones. They may also shame us into feeling bad about withholding data or declining options. Many times, companies make the ability to exercise control possible but costly through forced work, subtle misdirection, and incentive tethering.⁴ Sometimes platforms design online services to wheedle people into oversharing, such as keeping a “streak” going or nudging people to share old posts or congratulate others on Facebook. Companies know how impul-

³See Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

⁴For more information on the concept of dark patterns, see Harry Brignull’s <http://www.darkpatterns.org>.

sive sharing can be and therefore implement an entire system is set up to make it so easy.

Second, notice and choice regimes are overwhelming. They simply do not scale because they conceive of control and transparency as something people can never get enough of. People are gifted with a dizzying array of switches, delete buttons, and privacy settings. We are told that all is revealed in a company's privacy policy, if only we would read it. After privacy harms, companies promise more and better controls. And if they happen again, the diagnosis is often that companies simply must have not added enough or improved dials and check boxes.

Control over personal information is attractive in isolation. But often it's a practical and overwhelming obligation. While you might remember to adjust your privacy settings on Facebook, what about Instagram, Twitter, Google, Amazon, Netflix, Snapchat, Siri, Cortana, Fitbit, Candy Crush, your smart TV, your robot vacuum cleaner, your WiFi-connected car, and your child's Hello Barbie? Mobile apps can ask users for over two hundred permissions and even the average app asks for about five.⁵ The problem with thinking of privacy as control is that if we are given our wish for more privacy, it means we are given so much control that we choke on it.

One remedy policymakers have proposed is to make all choices privacy protective by default. However, even if the default works, ceaseless demands are still making us relent.⁶ Anyone that has turned off notifications on their mobile apps can attest to the persistent, grinding requests for the user to turn them back on almost every time they open the app. Many can relate to the experience of a child asking for candy, over and over, until the requests become too much to ignore and we give in, simply to quiet them. Willpower can feel like a finite, vulnerable, and subjective resource, and companies design systems to deplete and erode it. Once our willpower and ability to make choices has been compromised, the control we have been given is meaningless.

Even if a company achieves the platonic ideal of how to give data subjects' notice and choice, it wouldn't solve people's limited bandwidth dilemma. People only have twenty four hours in a day and every service they use wants them to make choices about how they can handle their data. Meaningful individual control over one data flow between a person and a data collector won't change the fact that the data ecosystem is vast. And it should be if the market is to be competitive. The modern data ecosystem is mind-bogglingly complex, with many different kinds of information collected in many different ways, stored in many different places, processed for many different functions and shared with many other parties. And even if every tech company merged together until only one giant tech company existed, the tension between simplicity and nuance in privacy policies would seem irresolvable. This is because when companies try to simplify and shorten information nuance is lost. Risk is either hidden in terms of use through abstraction or made so explicit and voluminous we don't even know where to begin.

The collective result of atomized online decisions is not the best guide for privacy policy. Research shows that peoples' privacy preferences are uncertain, contextually dependent, and malleable.⁷ The availability of knowledge doesn't necessarily translate into meaningfully informed decisions. People will always know less than companies regarding the wisdom of a decision. However, notice and choice regimes ask them to consider the privacy implications of each post they create and every action they take online—an impossibly complex calculation to make about future risks and consequences. In a world of predictions and group privacy, sometimes a person's consent is beside the point. For example, when members of my family consent to the practices of genetic testing companies by sending their DNA off for analysis, the DNA overlap implicates my privacy, but my consent is irrelevant.

Defending notice and choice regimes requires so much justification, so much stretching, bending, and tying ourselves in knots, that it feels like it's merely serving as a proxy for some other protection goal that is just out of reach. But it is not clear what the result that policymakers, industry, advocates, and data subjects are in truth hoping for. Control ostensibly serves autonomy, but in mediated environments involving personal data, idealizing control actually seems corrosive to autonomy. Is control valuable because people have such different privacy preferences? Or

⁵Kenneth Olmstead and Michelle Atkinson, *Apps Permissions in the Google Play Store*, PEW RESEARCH CENTER, (Nov. 10, 2015), <http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/>.

⁶Article 25 of Regulation (EU) 2016/679 on data protection by design and by default. [2016] OJ L119/1. See also Recital 78 of Regulation (EU) 2016/679.

⁷Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015).

does it just appear that way because personal data risks are almost impossible for people to assess?

If data processing is so dangerous that it requires formal permission, and meaningful choices can only be made in elusive, demanding, and bounded environments with preconditions such as “freely given, specific, informed, retractable, and unambiguous,” then it is worth asking why companies are allowed to engage in what feels like a fiction, even under optimal conditions. Is notice and choice just a contorted and indirect way to pressure companies to lay off risky data practices? If so, lawmakers should dispense with the pretense of demanding a form of notice and choice that seems destined to misdirect industry efforts towards formalistic compliance without a meaningful change in processor behavior.

B. The Fair Information Practices are Necessary But Not Sufficient

The push for consent and control partially springs from the original principles used to ensure fair data processing, referred to as the “Fair Information Practices” or the FIPs. These aspirational principles developed over the past fifty years are used to model rules for responsible data practices. They are the bedrock of modern data protection regimes around the world: Transparency of business practices; Access and correction rights; Data collection and use limitations; Accountability; Data minimization and deletion; Data accuracy; Purpose specification; and Confidentiality/security.

The FIPs provide a common set of values, which is necessary as data flows from one country to another at the speed of light. The FIPs provide a benchmark for industry, advocates, and policymakers to analyze new technologies. Privacy as a general concept is vague and understanding the stakes depends on a full account of the context at hand. But the FIPs are a little more concrete. This clarity gives everyone a more useful litmus test for determining whether companies are being responsible with people’s data. In short, the FIPs are invaluable for the modern world.

The FIPs have also painted lawmakers into a corner. A sea change is afoot in the relationship between privacy and technology. FIPs-based regimes were relatively well-equipped for the first wave of personal computing. But automated technologies and exponentially greater amounts of data have pushed FIPs principles like data minimization, transparency, choice and access to the limit. Advances in robotics, genetics, biometrics and algorithmic decision making are challenging rules meant to ensure fair aggregation of personal information in databases.

While the FIPs are a necessary as a component of a Federal Data Privacy Framework, they are not sufficient for several reasons. First, the FIPs have several blind spots. They are largely focused on data aggregation by industry. They do not directly contemplate peoples’ vulnerabilities to each other on platforms like social media, peoples’ susceptibility to manipulation, and issues of platform power. Anthropomorphized robots, fMRIs that measure brain activity, and advances in genetics raise problems like people’s susceptibility to things that look and act human, their inability to hide thoughts, and discrimination based on speculative predictions and forecasting of things that haven’t even happened yet. These problems are generally beyond the scope of the FIPs.

Often, traditional data protection frameworks are so focused on the individual that they overlook important social and civil rights implications of collecting and processing personal data. Marginalized communities, particularly communities of color, shoulder a disproportionate burden from privacy abuses.⁸ I would recommend frameworks that go beyond narrow and individualized conceptions of privacy to incorporate more societal and group-based concerns as well as civil rights-based protections.

We are only just beginning to see the human and societal costs of massive scale of data processing and platform dominance. In addition to core privacy related harms associated with data collection and data use, companies’ demand for personal information is negatively affecting our attention and how we spend our time, how we become informed citizens, and how we relate to each other. Phenomena like “fake news,” “deep fakes,” non-consensual pornography and harassment, oversharing on social media, addiction by design, and lives spent staring into our phones are at least partially attributable to or made worse by the personal data industrial complex. We need broader frameworks for personal data not just because information is personal to us, but because the incentive to exploit it creeps into nearly every aspect our technologically-mediated lives.

⁸The Leadership Conference on Civil & Human Rights, Letter to Senate and House Chairs Wicker, Graham, Pallone, and Nadler, and Ranking Members Cantwell, Feinstein, Walden, and Collins (Feb. 13, 2019), <https://civilrights.org/resource/address-data-driven-discrimination-protect-civil-rights/>.

The upshot is that existing data protection frameworks are important to build on, but they are still incomplete. That's why states play such a crucial role in the development of privacy policy in the U.S. Not only have states become quite involved in creating innovative privacy rules and frameworks, but they help carry the load of enforcement.

Legislation that preempts the states privacy regulatory and enforcement efforts would have net negative effects for privacy as well as jeopardize the international flow of data if U.S. privacy law appears weaker as a result. Diluted preemptive Federal law risks diminishing currently strong state rights and rules. State Attorneys General have played a key role in crafting and enforcing privacy rules.⁹ States have also shown a willingness to exercise new and innovative approaches to privacy law, including pioneering breach notification statutes and biometric privacy protections. Baseline legislation would follow the tradition of having the Federal government create a floor, not a ceiling, for privacy rules. Preemption of privacy laws is not the norm.

One temptation might be for lawmakers to seek a singular set of data protection rules to ease the cost of compliance. While harmonization of data protection rules into a national or even global standard would have benefits, an unwavering commitment to harmony with other regimes makes future progress difficult. Ossification of this sort would be fine if notice and choice were all the world needed to prepare for our future of algorithms and data. But U.S. privacy law needs more.

III. PRIVACY RULES SHOULD MOVE BEYOND CONSENT AND TRANSPARENCY

Notice and choice frameworks and overly-procedural privacy laws have resulted in a sea of blindly-clicked "I Agree" buttons, unread fine print, and constant anxiety about what our home Internet-of-Things device is listening to. What seems sensible on a case-by-case basis will in the aggregate continue to overwhelm people who simply want to be safe when they go online.

What the United States needs from Federal legislation is a set of rules that can rebalance the responsibilities of companies collecting, using, mining, and sharing individuals' personal data and protect against individual, group, and societal harm. Data collectors and processors are in the better position than we are to foresee how their tools and practices might be used in ways adverse to us. They are also in the better position to correct course.

The U.S. needs a set of rules with a firm commitment to many different privacy-related values. We should not treat privacy as a procedural and formalistic compliance exercise. We should not distill privacy protection into a rote checklist that allows data collectors to flash an insignia of compliance without making more substantive efforts to protect our vulnerabilities. To that end, I recommend rules structured to protect peoples' trust and rules that place robust, clear, and non-waivable boundaries around how information technologies are designed, what data companies may collect, and how that data may be used.

A. Trust Rules Can Help Create Safe and Sustainable Information Relationships

There are ways to balance utilizing data and protecting people, but it requires a framework that reimagines the relationship between people and the companies they interact with in a way that places trust at the center. Being trustworthy in the digital age means companies must be discreet with our data, honest about the risk of data practices, protective of our personal information and, above all, loyal to us—the data subjects.¹⁰ Our privacy frameworks should be built to encourage and ensure this kind of trustworthy conduct.

The United States needs to improve its poor international reputation regarding privacy. The world is watching, and the economic stakes are enormous. International data flows are essential for the global economy to function without fundamentally—and expensively—restructuring the Internet. American tech companies depend on being able to smoothly bring Europeans' data here for processing. But

⁹See Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2017).

¹⁰For more information on taking trust seriously in privacy law SEE ARI EZRA WALDMAN, *PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE* (2018); DANIEL SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 102–104 (2004); Ian Kerr, "Personal relationships in the Year 2000: Me and My ISP" in *NO PERSON IS AN ISLAND: PERSONAL RELATIONSHIPS OF DEPENDENCE AND INDEPENDENCE* (2002); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L. J. 1180 (2017); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law* 19 STAN. TECH. L. REV. 431 (2016); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

our current data-sharing agreement with Europe, the E.U./U.S. Privacy Shield, seems to be on thin ice. If it fails, we will need a good replacement grounded strong enforcement and effective, protective, and substantive rules.

Trust rules could not only help America establish its own robust privacy identity, but it can also serve to mutually benefit industry, people as individuals, and society at large by nourishing safe and sustainable information relationships. Concepts like “big data” and machine learning seem exciting to many. Data promises to revolutionize our work and finances, improve our health, and make our lives easier and better. But the scale and complexity of these concepts can also be scary and intimidating. The public’s paranoia should be understandable. We are perpetually unsure about organizations’ motives and methods. What do companies know about us? Are they keeping their insights safe from hackers? Are they selling their insights to unscrupulous parties? Most importantly, do organizations use our data against us? Like so many things in life, these relationships are a matter of trust.

In my research with Neil Richards, we have argued that trustworthy data stewards have four characteristics that promote trust: they are honest, discreet, protective, and loyal. Trustworthy stewards are honest because they forthcoming about the most important information for our well-being being, even if it might discourage use. Honesty rules place the obligation of being understood on the steward, rather than on peoples’ ability to scrutinize the dense, vague, and protean language of privacy policies and terms of service.

Stewards are also obligated to be discreet. They should they treat our data as presumptively confidential and sensitive. They should not disclose our personal data in ways contrary to our interests or expectations. Discretion involves robust de-identification efforts as well as nondisclosure.

Stewards have an obligation to protect personal data. They should hold the data securely against third parties, doing everything within reason to protect us from hacks and data breaches. Most fundamentally, keeping a trust requires loyalty. This involves data collectors putting the interests of those who trusted them with their data ahead of their own short-term potential for gain. Loyalty obligations would prohibit data collectors from, among other things, leveraging peoples’ own resource and cognitive limitations against them or engaging in unreasonable self-dealing when collecting and processing data.

To be effective, trust frameworks should also give regulators the resources they need to enforce privacy protections and prohibit companies from using dense terms-of-use agreements to get us to waive those obligations. Companies should be trustworthy regardless of what we “agree” to online.

B. Data Boundaries Can Restore Balance

The modern data ecosystem is a runaway train. Trust rules can help, but they will not be enough. Some practices might be so dangerous that they should be taken off the table entirely. Others might be harmful to society in ways that don’t implicate a violation of any trust. To be fully responsive to modern data problems, a meaningful Federal privacy framework needs to embrace substantive boundaries for data collection and use.

In some contexts, this might mean rules that simply prohibit certain practices. For example, lawmakers could outright prohibit collection or aggregation of certain kinds of data, such as biometric and genomic data. Lawmakers could mandate deletion. They could get serious about purpose limitations and requiring companies to have a “legitimate interest” in processing data. And in cases where technologies represent a grave danger to civil liberties, they should not rule out a moratorium or ban. Strong rules limiting collection and storage on the front end can mitigate concern about the privacy problems raised through data analytics, sharing, and exploitation.

Finally, without structural support, resources, and a strong political mandate for enforcement, any data protection framework will merely be a pretext for exploitation. Whether legislation creates a new data privacy agency or emboldens existing Federal agencies, regulators must have broad grants of authority, including rule-making provisions where necessary, robust civil penalty authority, and the ability to seek injunctions quickly to stop illegal practices. Individuals should have private causes of action and rights as data subjects.

IV. CONCLUSION

Lawmakers must leave notice and choice frameworks behind in order to meaningfully address privacy in the United States. Companies have consistently hailed strategies for increasing transparency and control as solutions to our privacy woes, but time and time again doing further exacerbated the problem. People need to be

able to trust the entities they deal with online and feel safe when they share information. Data protection rules should enforce that trust and create substantive boundaries in service privacy as well as more diverse values like civil rights, due process, and psychological well-being. If people and groups are protected instead of saddled with the risk of online interaction, our digital ecosystem can become sustainable.

BIOGRAPHY

Woodrow Hartzog is a Professor of Law and Computer Science at Northeastern University School of Law and the Khoury College of Computer Sciences. He is also a Non-resident Fellow at The Cordell Institute for Policy in Medicine & Law at Washington University, a Faculty Associate at the Berkman Klein Center for Internet & Society at Harvard University, and an Affiliate Scholar at the Center for Internet and Society at Stanford Law School.

His research focuses on privacy, media, and technology. His work has been published in scholarly publications such as the *Yale Law Journal*, *Columbia Law Review*, *California Law Review*, and *Michigan Law Review* and popular publications such as *The Washington Post*, *BBC*, *CNN*, *The Guardian*, *Wired*, *The Atlantic* and *The Nation*. He has been quoted or referenced in numerous articles and broadcasts, including *NPR*, *The New York Times*, *The Los Angeles Times*, and *The Wall Street Journal*.

He holds a Ph.D. in mass communication from the University of North Carolina at Chapel Hill, an LL.M. in intellectual property from the George Washington University Law School and a J.D. from Samford University's Cumberland School of Law.

He is the author of *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, published in 2018 by Harvard University Press.

The CHAIRMAN. Thank you, Dr. Hartzog, and thank you to all of our excellent panelists. Let us start then with preemption. We know that the GDPR, enacted by the European Union, went from something that was advisory to the various member states of the E.U., to something that became a regulation. And so, there was preemption in the E.U. We learned from Mr. Leibowitz that actually there was a patchwork of local privacy provisions in California and that State statute preempted the local. So, let me ask—let me start with you Mr. Leibowitz. Why is this important, and particularly with regard to our concern about consumers, why is Federal preemption something that you advocate?

Mr. LEIBOWITZ. Well, you always want to take the perspective of consumers, and I think Professor Hartzog made that point quite clearly. You do not want a cacophony or a crazy quilt patchwork of 50 different State laws. It will make consumers numb to notifications. If someone is driving from Biloxi, Mississippi to Bellevue, Washington, they do not want to go from State to State and have different regimes. And those regimes may be conflicting. And so—

The CHAIRMAN. I wonder if anybody has ever taken that drive. [Laughter.]

Mr. LEIBOWITZ. I am sure—you know I dropped a bunch of State to State references because I wanted to be under the 5-minute rule because I was told what would happen to me if I went over. But so, I am sure people have taken that drive, at least metaphorically, and I really—and it strikes us and our coalition, but really anyone and most importantly I think most people on the panel, is that you need to have one strong Federal privacy regime. It needs to be strong. It needs to empower consumers, but if you do that, then I think the right approach is to preempt State laws and make sure everyone is protected. And wherever you go, you are protected under that same tough rule.

The CHAIRMAN. Dr. Hartzog, if we allow the Federal law that we hope to enact on a bipartisan basis here to be a floor, doesn't that leave us with a patchwork? And where is Mr. Leibowitz wrong on that?

Dr. HARTZOG. Senator, it does leave us with a patchwork, but that is what we have been dealing with for quite some time. And I think that while consistency is nice, I think that the patchwork actually has been not something that has been insurmountable in so much as I teach my students to deal with 50 State patchworks all the time. As a matter of fact, we can—we are actually pretty good at dealing with that. And so, I think that to the extent that we are dealing with, 50 State patchworks as a problem—I do not see that as being insurmountable because it is what we have been dealing with all along when dealing with data breaches.

The CHAIRMAN. If you had been helping the E.U., would you have left it as it was with differences among the member states of the E.U.?

Dr. HARTZOG. Well, I think that that is a difficult distinction to draw because we are dealing with two entirely different systems and cultures. In the United States we have a tradition of dealing with a patchwork of 50 State laws, something that we have really been working with a while. And so, while I think there are virtues to consistency, in my opinion it is not the obstacle that would strike me as the first thing that we have to surmount if we are going to get privacy right.

The CHAIRMAN. Thank you. Ms. Espinel, about this distinction between controllers and processors, can you explain exactly what you meant there? What is the difference and exactly what are you advocating?

Ms. ESPINEL. Thank you. I would be happy to. So, first to be clear BSA companies act as both controllers and processors. And we believe that controls and processors should both have obligations, we just think the obligation should fit the role that they are in. So just to explain those terms a little bit, when a company is acting as a controller, they are controlling the data. That is to say, they are making decisions about how that data will be used, and we believe in that role, they should have primary responsibility. When a company is acting as the processor of a data, they are merely processing the data. They should still have obligations, but again, they should fit that role. So, for example, if they are processing the data, they should have an obligation to make sure the data is kept secure because that falls within the role that they are in at that moment.

I will add that one of the concerns that we have is that if exactly the same types of obligations are put on companies in both roles, you know as controller and as processor, we could actually end up undermining privacy protection. And the reason for that is because if you are acting as a processor, you do not necessarily have access or visibility into that data. If the same types of consumer rights and obligations on companies are put in there, you would put a processor in the position of having to go and get access to personal information that they would not necessarily have.

So, we think it is both important to make the law effective and workable, but we also think it is important because we think it

could undermine privacy protection if we do not make that distinction.

The CHAIRMAN. Thank you. Senator Cantwell.

Senator CANTWELL. Thank you, Mr. Chairman. I am—I was not really going to go with the preemption thing, but I just want to be clear since the chairman brought it up. I mean are we here just because we do not like the California law and we just want a Federal preemption law to shut it down? Or do people think you can have meaningful Federal privacy legislation without that? Just a yes or no from the witnesses.

Mr. LEIBOWITZ. No.

Senator CANTWELL. Thank you.

[Laughter.]

Mr. BECKERMAN. I think Congress can do better.

Senator CANTWELL. Mr. Dodge.

Mr. DODGE. We have advocated for Federal policy for some time prior to California, so we continue to do so.

Senator CANTWELL. So, you do not need preemption?

Mr. DODGE. We want Federal preemption—

Senator CANTWELL. Yes or no.

Mr. DODGE. Yes.

Senator CANTWELL. OK.

Ms. ESPINEL. We think there should be a strong Federal law.

Senator CANTWELL. But do you have to have preemption of States?

Ms. ESPINEL. We think that—again we think we can do better. We think California does not go as far as a Federal privacy law could go, and we do not want the privacy protection of a person to be dependent on the State in which they live. So, we think a Federal law would be better. And in doing that, should replace State laws that are not as clear and consistent and as strong as we would hope a Federal privacy law would be.

Mr. ROTHENBERG. Yes. Emphatically with an asterisk.

Dr. HARTZOG. I do not think preemption is necessary and I think it could be actively harmful.

Senator CANTWELL. Thank you. Dr. Hartzog I am a little more in your camp at this moment. I find this effort somewhat disturbing that with all the litany of things in privacy violations I just went through, and as countries are grappling with this, the first thing that people want to organize here in D.C. is a preemption effort. What we need to do is get at the task you just outlined, and Ms. Espinel you did a pretty good job too of outlining what are the challenges that we face. Let us get on the same page because I think us together getting on the same page about what are the consumer issues at stake here and how do we want to protect them, I think will get us a better result than just this focus.

First of all, I do not see my California colleagues acquiescing to the Congress on this issue anyways. So, I think what we need to do is be very, very clear here what our challenge is. Ms. Espinel, you mentioned fines and I am curious as to whether you think culturally that is the right message? We were very involved in setting standards on anti-manipulation after the Enron scandal, that is both at the FTC, CFTC, and the FIRC, and it was amazing to me how many companies thought they literally could be the owners of

home heating oil and keep it off the coast just to drive up the price. And you know, so I mean literally people said, oh yes that is within our rights.

Do you think we need a very bright line here that just creates the culture within various, you know, online developments that will help make a culture within companies aware that these are the risks and threats?

Ms. ESPINEL. Well, I think we need to have a culture where when companies are handling consumers? data or using in various ways what they are really focused on is the consumer. They are focused on the reasonable expectations of those consumers and very focused of that. And so, I think—I mean I think that will be a cultural shift at least for some companies.

Senator CANTWELL. Well you advocated an FTC fine and my point is, when you have this general counsel at your firm warning people that there will be a fine for doing these kinds of things, that is a pretty bright line. Dr. Hartzog do you have an opinion about this?

Dr. HARTZOG. So, I think that when we are thinking about these questions, its importance—the preemption conversation seems to lump a lot of different things together all at once, and it is worth sort of pulling them out. Not only are we talking about preemption as a way of consolidating possible enforcement efforts or maybe not, but there is also the question of the costs of disperse compliance and also—and I think that one of the reasons that I am really skeptical of preemption is that we are sort of operating under this assumption that we figured out exactly what all the rules should be.

Senator CANTWELL. I am referring more to Ms. Espinel's now point about giving FTC clear or fining authority. Is that a clearer, easier bright line to establish that would be helpful?

Dr. HARTZOG. Oh, Absolutely.

Ms. ESPINEL. In the first instance. And that I think also goes to changing the culture. Right now, in the first instance of a violation of Section 5, the FTC does not have fining authority. I think it will change cultures internally if companies know that for a first initial violation the FTC has authority that Congress will need to give them to be able to issue a fine against that—

Mr. LEIBOWITZ. And if I may add a point going back to your preemption question, Senator Cantwell. We would encourage, and it is your panel's decision of course, but we would encourage State AG enforcement. That is the approach on COPPA, which preempts but gives State AGs the ability to enforce the statute.

Senator CANTWELL. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. Mr. Rothenberg, could you explain your asterisk in 30 seconds?

Mr. ROTHENBERG. Certainly. Clearly you want consistency over chaos. That is the argument in favor of preemption, but equally clearly, there is an absolute role for the States to play in enforcement. And again, automotive safety is one of the many areas where you have Federal and State enforcement and regulations complementing each other, along with industry self-regulation. The trio is where you get the strongest opportunity to protect people's safety and privacy and security.

The CHAIRMAN. Thank you very much. Senator Fischer.

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

Senator FISCHER. Thank you, Mr. Chairman. Ms. Espinel, as Congress looks to strengthen the data privacy, it is crucial that we prevent irresponsible data use to begin with or on the front end, I think. As we look to define personal data, how it should be processed, and how a user might control their own personal data, what do you believe constitutes an unreasonable data use?

Ms. ESPINEL. Well I think a use of data that goes beyond the reasonable expectation of the consumer is inappropriate. I think that is—you know, there are some of those uses that could be worse than others, but I think that is really what we need to focus on. We need to focus on what is the reasonable expectation of that consumer and ensuring that companies are only using data in ways that lines up with that reasonable expectation. Another way of saying that is that, you know, companies should be limited to uses that are relevant to the stated purpose of why they are using the data. So, I think it comes back to the consumer and having that as kind of the central tenet of how companies are thinking about their data. Having that trusted relationship, I think, with your customer, with the consumer, is going to help motivate companies to do that.

Senator FISCHER. OK. I would ask each member the panel if you can give me one example of unreasonable data usage. For whoever would like to start.

Mr. LEIBOWITZ. Sure. When I was at the FCC, we brought multiple cases involving—dozens of cases actually—involving companies that made a commitment that we will keep your data private, and then they did not. That is deception. And then we brought a number of cases that involved companies that just had inadequate data security. That was such that they did not protect consumer data. But we did not have fining authority, you know, at the outset, I would say, which is something that our organization, 21st Century Privacy Coalition, supports.

Mr. BECKERMAN. Thank you. I would say if data is being used in a way that a person would be surprised about that use, in a way that is unexpected to them, in a way that does not benefit the consumer.

Mr. DODGE. Building off that, the relationship between retailers and their customers is about buying goods and services so anything that dramatically departs from that, in that context, would be a violation of the trust that is so important to retailers and their customers.

Ms. ESPINEL. So, I will give a concrete example to illustrate consumer expectation. I think when you put your location into a map service, it is your reasonable expectation that the map is going to use your location in order to give you directions. I think if you have a flashlight app that is tracking your location information, that is not something that a consumer, in my opinion, would reasonably expect, and so I think that would be an example of an inappropriate use in those circumstances.

Mr. ROTHENBERG. Senator, there are lots of examples we can give. Here—

Senator FISCHER. Just one.

Mr. ROTHENBERG. Here is one. It is, I am surfing the web or on an app where I am looking up recipes involving eggs and somehow that is going to insurance companies in order to deny me insurance or to raise the price of my insurance because it might have an impact on my cholesterol.

Dr. HARTZOG. An example that I would use would be the collection of things like biometrics that were used for maybe authentication devices that were then repurposed for things like surveillance across a wide variety of a context.

Senator FISCHER. OK. Good example. A core component of the GDPR is to guard against unreasonable uses of data through clear, explicit consent. However, in this case, we already are seeing interface redesigns that undermined user choice and the opt-out functions. We have numerous consent boxes that pop-up online or in applications, often with a threat that service cannot go forward, cannot be used unless the users is going to consent to it. Besides being really irritating to have that happen, I think we are left with an illusion of having some kind of control as users. Mr. Hartzog, do claims of complete user control incentivize users to share more personal data?

Dr. HARTZOG. Sure. I think they do. Who doesn't want more control? It sounds empowering and when you have it you feel like, OK, well now I want to interact here. But I think the problem with thinking about privacy in terms of control is that it is treated as though the mere gift of it is a protection of privacy in and of itself. When actually, if we cannot exercise that control, then it is meaningless, and it is overwhelming, and it is illusory, and I think that that is why I do not think that control should be the only value that we might be placing here, even though it seems to be—

Senator FISCHER. What do you want another value to be?

Dr. HARTZOG. Sure. Well, there are several you could think of. One would be trust relationships, right. So, things that encourage trust between people. There are values of dignity. There are other values. Control ostensibly serves autonomy, but it does not always sort of serve it. Obscurity, which is a value that we all sort of live in that that gets, you know, eroded over time that the control does not necessarily get at. I think that privacy as a broad concept, can include lots of different values. And it should not be distilled down to just control.

Senator FISCHER. Thank you. Thank you, Mr. Chair.

The CHAIRMAN. Thank you. Senator Klobuchar.

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

Senator KLOBUCHAR. Thank you. As you all know, I have privacy legislation with Senator Kennedy, bipartisan legislation, and in part, what I have found in getting involved in this is that the reason all the States are doing all this is that we have done nothing here. And part of it is because the companies that you represent have been lobbying against legislation like this for years. And it is never right enough, or they have got your backs, and it happens

time and time again. I encountered this with the Honest Ads Act, which some of the companies now support. But there is a reason the States are doing this, so let us not forget that when we talk about States and different patchworks of regulations.

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

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

Senator KLOBUCHAR. OK, so just, I have so many questions. You are not in favor of the 72-hours Mr. Beckerman?

Mr. BECKERMAN. It should not be exactly 72 hours because that might be impeding with an FBI investigation that could be plugging in the hole or going after the culprits. But they should be timely.

Senator KLOBUCHAR. OK. I am sure we could find some exceptions for that. So, Dr. Hartzog, in December the New York Times revealed that Facebook gave certain tech companies like Netflix, Spotify, Microsoft, Amazon, and others access to more user data, including private messages, without their explicit consent. Do you believe that companies are being fully transparent about sharing users' data with third parties?

Dr. HARTZOG. No. I think that is—and the problem is that there is a trap here, which is, you can either sort of be transparent with general abstractions and ways that are digestible and accessible, or you can sort of dump the entire volume of data practices on people, which would also not have the intended effect here. And so, while I think that transparency is critical, transparency to users might not be the right audience.

Senator KLOBUCHAR. OK.

Dr. HARTZOG. Regulators might be.

Senator KLOBUCHAR. Another issue is lengthy terms of service, complex language, which our bill also gets to. Mr. Beckerman, last month TechCrunch reported that two companies in your organization offered users, some as young as 13, either \$20 cash or gift cards to download research apps. Do you believe these users actually understood the terms and gave true informed consent?

Mr. BECKERMAN. I think terms of service that exists both on and offline need to be shorter and more simple, so people actually could understand. It does not make people more private or more secure, no matter what you are doing, if you need a law degree to read through 20 pages. And so we agree that these should be shortened down.

Senator KLOBUCHAR. So, you would like to see that as part of Federal legislation, to have plain language?

Mr. BECKERMAN. Absolutely. I mean companies need to have these short and concise so people can understand what they are looking at.

Senator KLOBUCHAR. And how about opting out of having personal information tracked and collected?

Mr. BECKERMAN. Yes, it is important that the tools that people have are contextual, and so you are able to not be surprised as you are using an app or service on how information is being used, and the control goes with the individual.

Mr. LEIBOWITZ. By the way, I just want to add, we support that.

Senator KLOBUCHAR. OK. And also, Mr. Leibowitz, our bill actually centralizes the authority to enforce a national privacy law with the FTC. And you believe that is right thing to do?

Mr. LEIBOWITZ. I do in my current capacity and I do in my previous capacity, yes.

Senator KLOBUCHAR. OK, well that means you do.

Mr. LEIBOWITZ. I do. Twice.

Senator KLOBUCHAR. OK, very good. The Honest Ads Act, I just want to go to that. Mr. Rothenberg, I know you represent 650 leading media and tech companies. Some of the companies have endorsed this bill. We now have 12 or 13 Republicans on the bill in the House, and we are working to replace Senator McCain, who we miss very much, so that we have some Republicans on this bill in the Senate given that all it does is require disclosure and disclaimers on political ads just like you have on TV, and radio, and newspaper. So, does your organization support the Honest Ads Act and greater transparency in political advertising?

Mr. ROTHENBERG. Yes, Senator, we do. We do have some reservations with some pieces of it because we think it potentially penalizes smaller publishers that are the, in effect, unwitting end nodes of the distribution of political advertising, while does not—it is not strong enough in identifying the complexities in the supply chain for the distribution of political ads. But, by the same token, we IAB have developed a mechanism for transparency for political advertising. It is the only one in the market place right now so—

Senator KLOBUCHAR. But don't you think we should have rules of their own in place, otherwise some platforms will do different things, or we are going to have the exact same patchwork that Mr. Leibowitz was referring to?

Mr. ROTHENBERG. Absolutely. We would love to have your legislation look at our political ads disclosure mechanism that is currently in the market and used as a safe harbor or a model for the kinds of things that ought to be done.

Senator KLOBUCHAR. OK. Well, I guess that we have 12 Republicans on my bill now in the House and so the hope is we will pass it there and I hope we can pass it here because 2020 is not far away. So, thank you very much.

The CHAIRMAN. Thank you, Senator Klobuchar. Senator Thune.

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

Senator THUNE. Thank you, Mr. Chairman. When I was Chairman of this Committee, we held a series of privacy hearings to begin the conversation on what Congress should do to promote clear privacy expectations, while ensuring that innovation and investment is not stifled. And so, I want to thank Chairman Wicker for making this a top priority of this committee, and I look forward

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

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

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

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

Senator THUNE. OK. And how would you go about formalizing that in a privacy law?

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

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

Mr. DODGE. Thank you for the question, Senator. Our members do view that as a concern, the lack of clarity around that and other

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

Senator THUNE. And this I just direct quickly to all the panelists. And that has to do with the question of whether or not you all support a technology neutral and sector neutral approach to Federal privacy legislation. And that is to say, should Internet service providers and edge providers be subject to the same privacy requirements, or should Federal legislation approach different business models differently? Whoever is willing to take that. Ms. Espinel?

Ms. ESPINEL. We think all companies should have strong obligations. I think their responsibilities should fit their role, but we think all companies should have strong obligations.

Senator THUNE. Does anybody disagree with that point of view?

Mr. LEIBOWITZ. No. And I just want to add, we agree. And going back to your earlier question, what can you do about the problems you raised, I think this committee has the opportunity to move a national bipartisan bill that would allow opt-in and opt-out in rights for sensitive data for consumers, opt-out rights for consumers, and strong enforcement of the FTC that would make sure that people do not do things that they know will cost them large amounts of money if they violate the law.

Senator THUNE. Well, I happen to believe that this is one of the areas, maybe not many areas in this next couple of years, that we ought to be able to come together around in a bipartisan way and come up with a national data privacy law that could be signed and enacted. And so, I hope that the discussions that we are having today will serve as a foundation for moving forward with legislation that gets out this issue because I think it is an important one to everybody in this country. It impacts literally everyone, so thank you all for being here.

The CHAIRMAN. Thank you, Senator Thune. Just quickly, Dr. Hartzog, do you agree with Ms. Espinel and Mr. Leibowitz on the tech neutral question?

Dr. HARTZOG. So, I think that there are virtues of tech neutrality, and in broad swaths, I think that it is advantageous. But I would actually caution against a sort of ceaseless commitment toward technological neutrality and sector neutrality just because I think it could be dangerous to treat all industries as though they have the same incentives and as do they do operate the same way. And so, I recognize these virtues, but we just push back against total devotion to it.

The CHAIRMAN. OK. Well you might want to supplement your answer there, and I appreciate it. Senator Schatz—

Senator CANTWELL. And if I could on that, Mr. Chairman, I do think that this is very instructive, particularly as it relates to what we did with HIPAA, and Gramm-Leach-Bliley, and all these. You know, we have taken sectors, the financial sector, we have taken the, you could even say, a little bit in the housing sector, but

health care, financial sector, and describe things by sectors on privacy issues, and it has let us—I am not saying that is the end-all and be-all. I am just saying, now we can look back at what we have done and how well did that serve us, taking that kind of approach. Thank you.

The CHAIRMAN. Thank you. Senator Schatz.

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

Senator SCHATZ. Thank you, Mr. Chairman. Thank you to all the testifiers. I want to flesh out this question of transparency and control because my judgment is that it is fine, but in an IoT universe and with lots of users being under 18, that it is just not practicable to expect that people are actually in control of all the dials that have to do with the internet.

And when you are taking about billions of sensors, devices throughout your house, Dr. Hartzog gave a few examples, but we are talking about by the time, you know, 10 years from now your toaster is going to be connected to the internet, your keys are going to be connected to the internet, and you are going to have—theoretically, if we just did transparency and control, you are going to have hundreds of micro decisions every day that you are supposed to achieve informed consent about and that is setting us == I mean, the practicability of that is a problem. But there is also this question of lots of kids use the Internet and will automatically click “I agree,” not knowing what they are agreeing to.

So, I am not criticizing transparency and control as something we should not do, but I am saying it is insufficient. And that is why I think we have to talk more about what is the obligation of a company once they are in possession of your data.

First of all, there is tons of data already in the possession of companies, so we have to deal with that problem. Second of all, people are going to click “I agree” irrespective of what the pros is, especially since everyone is going to be clicking “I agree” on some kind of 6-point font, while they are on the bus. And so, Dr. Hartzog, I want you to flesh out this duty of loyalty. This idea that when you go into the doctor’s office, they do not tell you to pick how that data is used. We are going to share it with the oncologist but not the nurse’s assistant. You just trust them. When you go into your lawyer’s office, it is not up to you to decide how that data is used. There is an affirmative obligation of the professional on the other side not harm you.

And so, I think any data privacy law has to have a backstop. Not just turning the dials, but an affirmative obligation for anyone that is in possession of your data to not harm you. And Dr. Hartzog, I wonder if you might comment on that.

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

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

Senator SCHATZ. Right. But it is—I just want to make the point, it is not just about the disclosure. They may disclose adequately—

Dr. HARTZOG. Right.

Senator SCHATZ. Even in plain language, even in a way that a 13-year-old can understand, I am not sure how that is doable but let us even stipulate that that is possible, still there ought to be obligations not to harm customers. I want to get to the FTC really quickly. My judgment is that we ought to have some broad principles and statute and allow the expert agency to flesh that out over time. And I think that includes rulemaking authority, first fine authority, and additional staffing. And I know that is kind of a lot, but you guys are all conversant in all this. Is there anyone who disagrees with rulemaking authority, first fine authority, and additional staffing to enforce this overtime? I will obviously start with our former FTC person.

Mr. LEIBOWITZ. Strongly support additional resources. The size of the FTC is the same now that it was a 1980—

Senator SCHATZ. I have 40 seconds, so I—

Mr. LEIBOWITZ. OK, fine. Strongly support more resources. Strongly support fining authority. Want to see what the Committee comes up with in terms of rulemaking, but some rulemaking with guardrails, I think we could support.

Senator SCHATZ. I will accept a yes for anyone who wants to be expeditious.

[Laughter.]

Mr. BECKERMAN. Definitely support more resources. On the rulemaking, there should be more direction from Congress on that and maybe a model similar to what we saw with COPPA would work.

Mr. DODGE. Support all three with a caveat of when we get to the end of this process, we will look at the legislation, to see where rulemaking applies.

Senator SCHATZ. Sure.

Ms. ESPINEL. Yes, we support targeted rulemaking. Yes, we support additional, new authority for additional fining, and yes, we support resources for the FTC so they can do their job.

Mr. ROTHENBERG. I agree with what the previous panelists have said.

Senator SCHATZ. Thank you.

Dr. HARTZOG. Yes, across the board.

Senator SCHATZ. Thank you.

The CHAIRMAN. Congratulations, Senator Schatz. Show of hands—no. Senator Moran.

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

Senator MORAN. Chairman, thank you. Thank you for you and the Ranking Member having this hearing. Thanks for our panelists for being here. Let me pick up on where Senator Schatz concluded. I believe that as we draft legislation that we need to provide clear and measurable requirements in statutory text for the FTC to utilize, while also including appropriate flexibility in narrow rule-making authority. And the goal there is to put the broad words in place that Congress believes is appropriate, and then to give the FTC authority to, as technology changes, for example, to make decisions overtime that narrow the scope. So, I think what I heard from all of you is that there would be agreement it that regard. You see value in having statutory requirements, and you see value in rulemaking authority by the FTC, and I heard a caveat at least with one of you which I think it makes sense to me. It does make sense to me that the guardrails are necessary in regard to that rulemaking authority. Anybody want to contradict what I think you all are agreeing to?

[No response.]

Senator MORAN. Good. Then second, the question of fine. The ability to impose fines. So that makes sense to me as well, but let me have you explain for me how you think that civil authority should work. One of the suggestions that the GAO made to enhance Internet privacy oversight was civil penalties for first-time violators. This was a report that GAO published last January and again, I think I heard all of you say that you would be supportive of that kind of authority. Although I would not be surprised if some of you would want to tell me what that fine authority ought to be? Just broad fine authority. Want to narrow it down?

Mr. DODGE. I will just say, you know, we want a high-level standard, national standard and we believe for it to be effective, it has to have teeth, which means giving the FTC the authority to fine in the first instance.

Senator MORAN. And then, Senator Schatz talked about the resources necessary. I am a member of the Appropriations committee that funds the FTC. Maybe this if for you, Mr. Chairman, chairman Leibowitz. When you say additional resources, what does that mean? Senator Schatz said staffing. What is missing at the FTC to do—maybe the resources are inadequate today, but as we add greater authorities, what is required?

Mr. LEIBOWITZ. Well, look you do not want the quality of the agency's work to be strained by the quantity of demands placed upon it. So that is at a high level. At time a more granular level, the number of FTEs at the FTC is right about where it was in 1980. The population of the United States has grown by a hundred million since then. We are talking about the most complex issues involving online data, when you are doing investigations.

So—and the budget has been flat since I was there in 2010. And so, you need to give the commission, I would say, more resources. I do not think you want it like—I do not think you want to say overnight double the size because you cannot do that. You want to grow it thoughtfully, but I think if you—our belief, collectively and unanimously of the commission, was that if you could grow the

commission number of employees by 10 percent a year over a period of time, say 5 years, that would be enormously helpful.

Senator MORAN. Let me make certain that I also understand that it is the FTC that we believe should have these authorities. Statutory authority should be granted to the FTC, civil penalty aspect to the FTC. I think when we started this conversation, whenever that was years ago, overtime it seems to me that there has been a consensus growing about the FTC being the appropriate place to house the authorities we are talking about. Any disagreement from any of you in that regard?

Ms. ESPINEL. No. I would just add, we also believe the FTC should be the primary enforcer of Federal law, but we additionally would support having State Attorneys General have the ability to enforce on behalf of residents of their State.

Senator MORAN. I want to admit, I think I misunderstood you. You said the FTC not the FCC?

Ms. ESPINEL. The FTC.

Senator MORAN. You said FTC, correct?

Ms. ESPINEL. Mr. Leibowitz's former agency.

Mr. LEIBOWITZ. FTC. But we also support State Attorneys General, and in COPPA, that is the regime that Congress gave to the FTC. The FTC enforces and State AGs enforce.

Senator MORAN. OK. Thank you, Mr. Chairman.

The CHAIRMAN. And thank you, Senator Moran. Senator Markey.

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

Senator MARKEY. Thank you, Mr. Chairman. Both Europe's and California's new privacy laws acknowledge a fundamental principle, the children and teens are vulnerable populations that deserve special, unique protections. Europe identifies children as vulnerable individuals who deserve specific protections, and under European rules that are already in place, there is a heightened measure for a 13, 14, and 15-year-olds. While California's law establishes an opt-out standard for adults, it includes an opt-in standard for users under 16.

These laws reflect emerging consensus that kids and teens are growing up in a world in which their personal information is a valuable commodity, so we must construct meaningful guardrails. As the Committee develops a comprehensive privacy bill, we should institute special safeguards for 13, 14, and 15-year-olds who right now have no protection under the law. Mr. Leibowitz, do you agree that Congress has historically acknowledged on a bipartisan basis that kids are a vulnerable population deserving of special rules?

Mr. LEIBOWITZ. Yes, I do. And I think we see that in COPPA.

Senator MARKEY. Yes. So, I am the author of COPPA, the Child Online Privacy Protection Act, the constitution for children's protection in our country. Ms. Espinel, do you agree that COPPA is critical in protecting young people's privacy online?

Ms. ESPINEL. We do, and we thank you for your many years of leadership.

Senator MARKEY. So, now we have to update it. So, which is a starting point. It is up to 12 and under in COPPA. Now we have to go to the Facebook era, now that we live in, and 13 and 14 and

15-year-old's data are being compromised. So, Mr. Hartzog, do you agree that a comprehensive Federal privacy bill should include special protections for children 13, 14, and 15?

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

Senator MARKEY. Should it be opt-in?

Dr. HARTZOG. Yes, I believe so.

Senator MARKEY. You agree with that Ms. Espinel?

Ms. ESPINEL. I think our hope is that we end up with a Federal privacy legislation that is so strong that it will adequately protect everyone.

Senator MARKEY. But a minimum for kids is opt-in regardless of what we do for adults. Do you agree with that?

Ms. ESPINEL. So, I think we think sensitive data for anyone should be opt-in, and we have a pretty broad definition of sensitive data—

Senator MARKEY. I agree with you on that. I am agreeing with you. I am just trying to carve out one—

Ms. ESPINEL. But in terms of distinctions between 30 and 16, I will say this, I completely understand where you are coming from. I think we would like to have more conversations with you about that.

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

Mr. LEIBOWITZ. I would say at the very least opt-out for 13 and up, and we want to work with you on any legislation you would like to incorporate into the larger bill.

Senator MARKEY. OK. Thank you. Well, how about you, Mr. Rothenberg. Opt-in for kids?

Mr. ROTHENBERG. It is the same answer as Ms. Espinel and Mr. Leibowitz. Obviously, as a principle, clearly. Devil is in the details. I worry about blanket prohibitions on all communications to 15-year-olds or 14-year-olds.

Senator MARKEY. It is not like a prohibition. It is just opt-in. Again, we look at the California law and European law. So, kind of we preempt, and we make it lower than that.

Mr. ROTHENBERG. Yes, again—

Senator MARKEY. It would cause a big problem if we lowered their standard.

Mr. ROTHENBERG. No. Again—

Senator MARKEY. So, I am just putting that out there as the reality of it, and to make sure that we take kids and put them out of bounds, in terms of just having the extra special protection. The bill also includes an eraser button for kids by requiring companies to permit users to eliminate publicly available personal information submitted by the child. That is already, again, the law in California. Mr. Hartzog, you have written about the importance of allowing users to delete content that they posted as children from the internet. Why is that so important and should we build that protection into the law?

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

Senator MARKEY. Yes. And on the question of discriminatory use of information, men and women differentiated, other categories, do you think we need to take account of that in any law that we pass so that we do not have that discriminatory contact out of line, Doctor?

Dr. HARTZOG. I would agree with that.

Senator MARKEY. Thank you. OK. I thank you, Mr. Chairman. Again, kids have to be given an extra level of protection. They are vulnerable. They are targeted, and without building that in, I just think that makes no sense to preempt California or anywhere else. Thank you.

The CHAIRMAN. Anybody want to disagree on the eraser button? [No response.]

The CHAIRMAN. No one. OK. Senator Blackburn.

**STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE**

Senator BLACKBURN. Thank you, Mr. Chairman. Thanks for calling the hearing, and I have to tell you, it is like reliving old times to sit here and hear Ed Markey talk about these issues. We did this in the House for years as Mr. Leibowitz remembers well, and I am sure Mr. Beckerman too. It was in 2013 we started working on privacy and data security in the House and trying to push toward a national standard for privacy and push toward some data security provisions. Of course, 2014 was the year of the breach. We realized that it needed to be done, so hopefully we can help the Senate now cross that. Ms. Baldwin with us, she was there in the House as we debated these at Energy and Commerce.

I do think that it is important that we get these rights, and that we do it right. And that we not give people a false sense of security. And that is the reason that I led the push to get rid of the FCC's 2016 privacy order because I felt like that did give a false sense of security. I also introduced one of the first bipartisan, certainly the first in the House, bipartisan bill on privacy, The Browser Act. And Mr. Leibowitz, I loved your comments. You kind of went through all the provisions that are in that bill. And as we work on a product here, I do hope that those standards are included and that we do have, Ms. Espinel coming back to your comment, one set of standards for the entire ecosystem because that provides clarity and it helps raise consumer awareness. I want to talk for just a minute.

Mr. Beckerman, I am going to start with you, and I know you have seen all the articles that have been in the press lately about the app developers sharing sensitive data, sensitive information with Facebook and others. There was also the Cambridge Analytica issue. We now have the Nest issue. So many scandals. And I think that you would agree, and probably all of you would agree, we now realize this data sharing is not a bug. It is a business. It is a business model. And big tech has made a whole lot of money by exploit-

ing the use of this data. And it is one of the reasons that we have to come together. We are glad to hear you all say you are going to come together and work with us on it because as Ms. Klobuchar said, you have spent a lot of money fighting this. And that goes back to 2013 when we started on this.

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

Mr. BECKERMAN. Thank you, Senator and thanks for your leadership on this issue for many years. Consumers deserve more and we want to make that very clear. We support this bill, and as you have noted, you know, this is an online and offline, all the apps, all the companies, everybody should be part of this, and people should get more.

Senator BLACKBURN. OK, so then what are you doing to encourage these companies to be more transparent and to provide more protections? Because it is nice to come in here and talk about what we are going to do. You all have been doing this for years. But we are not seeing the action in the protections that are embedded in these processes.

Mr. BECKERMAN. Absolutely. I mean, and while we do need a Federal approach that preempts the States that we talked about to get it right for both small businesses and individuals, our companies are taking steps every day, adding new tools and new ability for people to delete their accounts, delete information, bring information between services to all the things that we are talking about in our principles, are things that are being rolled out in many of our companies.

Senator BLACKBURN. OK. So, every one of you, each of you, have talked about trust and having trust with individuals that their virtual you is protected online. So, Mr. Beckerman, what are your people doing? And when you talk about trust as a priority, is it or is it not, is it a top priority, is it middle of the way, do you just give it lip service? How are you approaching that?

Mr. BECKERMAN. Trust is number one. If people do not feel secure—

Senator BLACKBURN. They do not trust you now. So, what are you doing to—

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

Senator BLACKBURN. We will look forward to some positive actions. I yield back.

The CHAIRMAN. Thank you, Senator Blackburn. Senator Blumenthal.

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

Senator BLUMENTHAL. Thank you, Mr. Chairman. Let me begin by thanking the chairman for having this meeting. Also, Senator Thune for his work before now, and thank both the Ranking Member, Senator Cantwell, and Senator Wicker for their leadership in this area. What you have heard here is profound distrust on both sides of the aisle with the situation that exists right now. In a sense that we have passed whatever the turning point is for Congress to act. We have been working diligently. Senator Wicker, myself, Senator Schatz and Senator Moran on solutions here, and we enlist and urge your participation.

But simply to second what Senator Klobuchar said, you have to convince us that you really want something more than preemption. You have to convince us that your clients really want change in this area because the overwhelming evidence so far is that they are willing to look the other way. To put profits ahead of people here. And so, I think that we have a trust gap that we need to bridge. And most consumers simply have no idea about the vastness of their vulnerability because they have no real comprehension about how much data is collected, whether it is their locations, through all kinds of mechanisms that exist to track them, or the voices of their children through toys that they use, or biometrics that are gathered in the name of security.

The depth and breadth of data collection is like a vast galaxy out there, unknown to most consumers. And I want to urge you to, in effect, put your money where your mouth is. I do not mean that disrespectfully in any way, but we all know that the industries involved here have a record of looking the other way or ignoring their obligations in the specifics, the nuts and bolts, the granular efforts that are required. Let me begin by asking, how many of you believe that Americans deserve the same level of privacy now, as a floor, that California provides for its people? You can just raise your hand. How many of you feel that California ought to be a floor not a ceiling?

Ms. ESPINEL. We believe it is a floor. We believe that strong Federal privacy legislation could go beyond California and improve on California.

Mr. BECKERMAN. Senators, that is a great question. To be perfectly clear, the Federal bill needs to be worthy of preemption, and we are not talking about weakening California. What we are looking for is something actually that gives people more and better, and more meaningful privacy than what California does, and there are things in the California bill, as has been pointed out, that actually make people less private. And we think this committee and Congress can do better. Make something that is more private than what California has.

Senator BLUMENTHAL. So, it should be a floor not a ceiling?

Mr. BECKERMAN. Sure.

Senator BLUMENTHAL. It should be stronger than California.

Mr. BECKERMAN. Stronger than California, yes.

Senator BLUMENTHAL. Do you agree, Mr. Leibowitz?

Mr. LEIBOWITZ. We believe stronger and better.

Mr. DODGE. We would agree. We think it is very instructive in setting Federal standards.

Senator BLUMENTHAL. Instructive as a—

Mr. DODGE. Instructive as a—

Senator BLUMENTHAL.—floor, so it should be even tougher?

Mr. DODGE. There should be a high standard—

Senator BLUMENTHAL. Well, I am asking you—

Mr. DODGE. Yes, of course.

Senator BLUMENTHAL. You can say no, but do not tell me it is instructive, tell me whether you think it is the minimum as a floor.

Mr. DODGE. The absolute sentiment of the California law is to give strong control of users and transparency, which we fundamentally agree with. We could quibble with some things on the edges, but I do think it sets a very high standard and would be a good floor for Federal legislation.

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

Dr. HARTZOG. I would agree though. I would focus on the fact that the preemption is not just about providing sort of better more or less protection, but also about questions of nimbleness and ossification. And so, I think that treating California as a floor is a start, but that that is not the entirety of the preemption debate.

Senator BLUMENTHAL. What we really need is a privacy bill of rights that is expansive and flexible. Just like our constitutional Bill of Rights is. Correct? Thank you all.

The CHAIRMAN. Thank you, Senator Blumenthal. Senator Capito.

**STATEMENT OF HON. SHELLEY MOORE CAPITO,
U.S. SENATOR FROM WEST VIRGINIA**

Senator CAPITO. Thank you, Mr. Chairman, and thank all of you for being here. We have had several hearings, and Mr. Chairman I appreciate this one. Here is a question I have wondered, and I will start with Mr. Beckerman just because I think that might be a natural start, but I would like to hear from all of you. In our committee hearings we have heard a lot of pushback on the GDPR, and then some confusion with the California law as well. You just now, all of you, advocated for better and more stringent, is the way I heard it, more stringent privacy parameters than what is offered under the California law. But in an international company, and I believe this to be true, even if we set a standard here, you still have to comply with the GDPR. Am I correct?

Mr. BECKERMAN. Yes, Senator. Thank you. I mean, this is an important point too. It is important that we have a system that is interoperable with GDPR and that is one of the, I think, criticisms from many about GDPR is that it is very, very expensive to comply with and very complicated where a lot of small and medium-sized businesses have decided that they are no longer able to do business in Europe because of this law. And I do not think that is a model that we want to take here, and is another reason why having one

Federal strong approach that small and medium-sized businesses in every State can comply with in an easy way without having to hire teams of lawyers to comply with is a better approach.

Senator CAPITO. Yes, so I guess my point is with the larger companies that are still remaining to do business globally in the E.U., that—you are already complying with that standard, complicated or not. You are going to have to keep complying with that standard, complicated or not. So, I do not know, maybe I am looking at this the wrong way, but I mean, and I certainly do not know all the weeds of all the regulatory things in the GDPR, but would it in the end be simpler and easier for ease of business to have that standard be the standard for the company that is already getting applied to rather than have two separate standards?

Mr. LEIBOWITZ. If I could take that, Senator Capito. In some ways it might be simpler, but it would not be better. And so, as you are designing a framework, what you want to do is make sure that you have the benefits of stronger privacy protection and there is a clear consensus on this panel that is what you want to do, and it is bipartisan. And that is great. But you also do not want to undermine innovation.

So, for example, there is some early reports that suggest that innovation has slowed down. New business models have slowed down. The LA Times pulled out and so did Pottery Barn, pulled out of European—pulled out of Europe because they do not want to have to comply. So, I think you want strong privacy protections. I think if you want more trust from companies, you need a strong Federal backstop. You do not want multiple clicks away, but then you want to design legislation that is going to allow for innovation, while also protecting consumers.

Senator CAPITO. Thank you. I would say, you know, I joined the course of the bipartisan support for consumer privacy. My question—I am going to go then, how do we guard against, in creating this new standard here in the United States, how do we guard against what we already see has happened in Europe? And that is the smaller businesses that can no longer comply. How are we going to guard against that in terms of creating this new standard? What challenges does that bring as well? Does anybody have a thought?

Mr. ROTHENBERG. Yes, Senator. As I have been saying, I think consistency built on right principles and actual mechanisms will allow the clarity for smaller businesses to remain competitive. In your question—

Senator CAPITO. Without the high cost?

Mr. ROTHENBERG. Without the high cost. Your question to Mr. Beckerman began with the referencing larger companies and what they do with this, but that is the problem. Larger companies will always have the resources to be able to invest in this, we just have to be cognizant. We have scores and scores of newspapers that we know of that have pulled out of Europe because of the cost of compliance with GDPR.

Senator CAPITO. Right. I also appreciate the conversation on the youthful children and young teens being able to have some more protections, but, you know, at the other end of the age spectrum there are issues as well. And I think as we all age, we are going

to be reliant on our Internet capabilities a lot more than say the generation who is 85 to 90 now. And we know that scams around seniors are prolific in just about every household. I do not know how you think about it, but think about that when you are putting together your standards because I think that could bring about a—you know, I do not even want to say a country but the country writing to your grandmother saying you have got \$5,000 but you have got to send me \$1,000, you know. And now this grandmother knows how to do it. So, I think that is the difference and I would caution all of you as you are helping us to develop this, to make sure we guard against that. Thank you.

The CHAIRMAN. Thank you, Senator Capito. Senator Rosen.

**STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA**

Senator ROSEN. Thank you. I really appreciate the testimony today. I have a couple of questions, but one thing that nobody has talked about is data center security. So, one of the things that, you know, they are the keeper of all this data that everybody is collecting.

So, when we think about privacy, we do not often—you are not talking about where the data is actually stored. How it is stored and protected, and in Nevada, of course, we are home to some large data storage sites, and I want to be sure that in the framework that we talk about where it is stored, protecting it from physical attacks and cyber security attacks. So, my question is, what are some of the ways your organization thinks about physically securing these data centers? What they might do, how long they keep the data, and what happens potentially to orphan data if companies go out of business? It still is stored and even the data security companies have backup upon backup upon backup. So how are you going to address this in the privacy issue?

Ms. ESPINEL. I will start and then there may be other panelists that want to jump in. So, you know, for our companies, this is at the core of what many of them do. Their business model, the business that they are in, is protected with security of data.

So, it is an issue that our companies have thought about for a long, long time, and we are in support of that if there is privacy legislation passed, that as part of the privacy legislation actually includes specific obligations on securing of data because it is such an important issue in this context. It is one that Senator Cantwell raised as well at the beginning of this hearing and we think it is critically important that it be part of, not just the privacy debate, but we would hope it would be part of Federal privacy legislation.

Mr. ROTHENBERG. Senator, if I could jump in too and just build on that. You are noting an essential point. We look at this as a, centrally, a supply chain management issue. It is the porousness of the digital media marketing, advertising services supply chain that creates these problems. In that sense, you cannot separate security from privacy even though they are two different things. So, you have to put them together.

One of the mechanisms that we have built with our sister trade associations is called the Trustworthy Accountability Group. It is based on an auditing regime, not just a compliance regime, but an

auditing regime to help assure that your supply chain partners are trustworthy when you pass data to them. It is based on auditing and it has had a demonstrable impact on reduction in advertising-based fraud, delivery of malware, those kinds of things. So, we are in favor of building stronger supply chain protections into the law.

Senator ROSEN. And could we please be sure that we talk about orphan data as companies go in and out of business, that it is still stored some place?

Mr. ROTHENBERG. Yes, it is a very important point. Thank you for raising it.

Senator ROSEN. Someone else want to answer that?

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

Senator ROSEN. And I want to interject one other thing. Do you think it would be important for us to label some of these large data centers as critical infrastructure, just like we do other parts of our grid? Anyone want to answer that?

Ms. ESPINEL. I do not have an answer. I think we would be happy to think about it.

Mr. LEIBOWITZ. Yes, and we know you have an IT background and we would be happy to work with you. I would also just say on the notion of data security, we have supported legislation for stronger data security standards since 2013. I think only about a dozen States have laws and there should be a Federal standard.

Mr. DODGE. And just adding on to that, we have long advocated for Federal data security standards, universal breach notification rules. We think it belongs—it is the other side of the coin to privacy for sure, and we think that the obligations in it should extend to third parties as well.

Dr. HARTZOG. And I will just jump in and say that while security is distinct in many different ways by the ways we craft rules and maybe privacy frameworks, they are related so intimately. I mean it is worth thinking about how your appetite for data creates security problems and how we might think about rules that actually start getting at limiting the appetite and collection rules. Or deletion rules as well.

Senator ROSEN. Thank you.

The CHAIRMAN. Thank you, Senator Rosen. Senator Lee.

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

Senator LEE. Mr. Leibowitz, I would like to start with you. When we look at the internet, we are examining something that did not exist at the founding, but it is important to evaluate what kind of thing it is so that we understand our own regulatory power relative to that thing. You can analogize it to a channel or instrumentality of interstate commerce. You know, the Internet did not exist 250 years ago. Channels and instrumentalities of interstate commerce

certainly did. In light of the fact that it is a channel or instrumentality under this theory, how would you describe the scope of Congress's authority over the internet? Would you describe it as exclusive?

Mr. LEIBOWITZ. I would not—well, I would describe, I guess, the better architecture and this goes back to the commerce laws. It goes back to *Gibbons v. Ogden*. I would describe the better architecture as a strong Federal law or strong Federal laws—we are talking about privacy but there can be others—that sets a single high standard for consumer protection. And of course, it is integrally involved in interstate commerce.

Senator LEE. And State Governments of course have a legitimate interest in regulating a number of things. Things that might incidentally touch the internet. So how do we as a Congress balance the need to operate on this interstate channel or instrumentality of interstate commerce, while not trampling over their authority?

Mr. LEIBOWITZ. Well, that is a fair point, and you know, we all believe in States' laboratories of democracy. But we do not have State by State seat belt laws. We do not have State by State FAA laws. California, when it passed its own State law, which proved that lawmakers can protect consumer privacy, preempted all of the municipal laws that existed.

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

Senator LEE. Thank you. That is helpful. There has been a lot of discussion about the FTC's rulemaking authority. It is authority under the APA to make rules curing the force of generally applicable Federal law. Now when Congress delegates broad regulatory powers to an agency, subsequent rulemaking can create some unintended consequences because what is in effect happening is that that agency is making a law. And sometimes it can become difficult to reverse the burdensome impact that might have on a particular industry.

Mr. Leibowitz, I am concerned about overly prescriptive privacy regulations and the impact that they have the potential to have, particularly in the area of competition. Do you think that laws and regulations, and even some rulemakings by the FTC, could have a potential GDPR-like impact on competition, by insulating big market incumbents against competition and posing additional barriers on entry?

Mr. LEIBOWITZ. Well, I think you always worry about any rules or any laws that create new barriers to entry. We have seen that with GDPR. I would say that this committee, and we will see where your legislation comes out, could give any rulemaking authority to the FTC under some guardrails. For example, in COPPA, where you gave some delegation, but a limited delegation, to the FTC. They were not allowed to increase the age from 12 to 14 of COPPA, but they were allowed to determine what constitutes sensitive information.

So, in 2012, when we updated COPPA because COPPA was passed up, as Senator Markey was one of the authors, was passed

at a time when we did not really know what the Internet would do. We made precise geolocation a sensitive category of information. But you could also come up with a lot of the sensitive categories of information yourself if you wanted to do that.

Senator LEE. Right. In some ways, an agency like the FTC could be said perhaps to be operating at its best when it is playing the role of cop rather than lawmaker. Enforcement actions rather than new rulemaking endeavors can be helpful, and they also help increase rather than diminish certainty within the industry. Would you agree with that?

Mr. LEIBOWITZ. Well, so, then of course you have oversight within your subcommittee over the FTC and have served some time, so you know the agency well. We think of the agency or people at the agency think of it as first enforcement agency, second, a policy agency, and maybe third, a rulemaking agency when Congress clearly delegates that authority for rulemaking. That is why Congress put the FTC under the Magnuson-Moss Act, which makes it very hard to do general rulemaking without an APA delegation from Congress.

Senator LEE. Thank you very much, Mr. Leibowitz. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Lee. Senator Baldwin.

**STATEMENT OF HON. TAMMY BALDWIN,
U.S. SENATOR FROM WISCONSIN**

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

While our hearing today was spurred by stories of data misuse, like the Cambridge Analytica scandal, I am not sure that my constituents differentiate between a company's decision to use their data or give it to others in ways they did not expect or agree to, and a company's failure to keep that data secure from third-party criminals who want to steal it. The folks I heard from were just as outraged by Equifax as they were with Facebook. So, Dr. Hartzog, if you are going to do something aimed at making Americans feel that they can trust these companies with their personal data, do you agree that setting standards for both security of that data, should be part of this conversation on the privacy and unexpected use? And I am interested also in what other panelists might say about tackling both.

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

Senator BALDWIN. Anyone else wanting to share?

Mr. BECKERMAN. Sure. I agree. I mean, privacy and security of data are two sides of the same coin. And it is just as important, maybe in some cases, more important. In one area where this has not come up yet, in the context of this hearing, is also Government use. And we have seen time and time again a lot of very large breaches and hacks of Government data of personal information of individuals that have major consequences, and that needs to be part of it, as well as privacy from the Government. Governments at all levels, as you know, State, local, Federal are often making very broad data requests of companies and it is not always clear how that fits into law, due process. And then also data and cyber security. You do not want to have a case where companies are turning over data to the Government just to have it leak out in a hack or something. So that also needs to be addressed as part of this.

Senator BALDWIN. OK.

Ms. ESPINEL. Can I just actually add one caveat—

Senator BALDWIN. Yes, please.

Ms. ESPINEL.—detail to that. So, the companies I represent, many of them are in the cyber security business. This is very important to us. We have long advocated for data breach legislation. We have actually advocated in this context that we have legislation on data security be part of this, but I will say that while we think that would be optimal, we would also not want to see privacy legislation not happen if data security or data breach became the issue. We do not need them to move together. We think that would be best, but our number one priority is strong, clear, consistent, workable, effective, truly strong Federal privacy legislation.

Senator BALDWIN. Thank you.

Mr. DODGE. I would fully agree with that. Just add to it that the whole objective here is to put customers at the center of all of this. To give them a clear understanding and expectations around how data is being used, and they should have a clear level of confidence around how it is being protected. So, the two work together very importantly.

Mr. ROTHENBERG. I think there is an important point that you referenced Senator. It is that where people intersect the most with actual harm is based on various forms of data breach not privacy breaches. It is phishing e-mails. It is—and I do not want to minimize anything about privacy, but I would say that where people get hit in their pocket books right now are in very simple scams that are based on data leaking to places it should not leak to.

Senator BALDWIN. OK.

Dr. HARTZOG. Though I would also push back that an obsession over data security harms too much. I think, pulls us away from, I think, a more holistic sort of protection for privacy laws.

Mr. DODGE. I would agree.

Senator BALDWIN. Thank you.

The CHAIRMAN. Thank you, Senator Baldwin. Senator Young.

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

Senator YOUNG. I thank our witnesses for being here today. I am going to ask a question to Mr. Leibowitz, but I will submit it to everyone, so you have an opportunity to respond in writing. But there is two things that I would like to get to. First one, and we will touch briefly on it, Mr. Leibowitz, it is related to the treatment of different types of information.

And then, more importantly I would like to get to developing a Federal data privacy framework that does not disadvantage our smaller entities, small businesses, and startups, and so forth. So, there are clearly different types of information. There is location tracking information. There is DNA information. There is birth certificates, date of birth, personal identifiers. So, Mr. Leibowitz, should Congress create a Federal data privacy framework that treats the same information differently depending on who has control over that information, or should it instead focus on the actual nature of the information regardless of who is in control?

Mr. LEIBOWITZ. So first of all, Senator Young—

Senator YOUNG. Or is that a false choice?

Mr. LEIBOWITZ.—no, it is not a false choice. But first of all, I just want to say I am glad you did not want to ask me about the Indiana-Wisconsin game last night.

[Laughter.]

Senator YOUNG. That would be a longer conversation.

Mr. LEIBOWITZ. Anyway, so I think it should be—look, the right approach is technology-neutral. We should not obsess about that, as Professor Hartzog mentioned, but that is the right approach. It should not be about who collects the data, but what data is collected and how it is used because from the perspective of the consumer, that is what they care about and that is what they should care about.

Senator YOUNG. So how it is used, I would infer from that, that is very much related to who controls the information.

Mr. LEIBOWITZ. That is correct.

Senator YOUNG. OK. All right, thanks. Again, I will give all of you an opportunity to respond in writing. So, the next line of questioning you are anticipating. So, post GDPR, there is actually an economic working paper. Again, a working paper, so it is not done yet, but it appears to indicate there has been a significant drop in investments in startups, small businesses, and the like post GDPR. While at the same time, large incumbent enterprises have increased their market share. Now if in fact this turns out to be the case, and we continue to get more information that reinforces this dynamic, it seems that we might too run the risk of harming small businesses and new startups, and further entrench larger incumbents for years to come if we create a Federal privacy law that is difficult and burdensome to comply with. So how best can we tailor our standards so that small businesses and startups are not disadvantaged by our new standards?

Mr. LEIBOWITZ. So, I would say a few things. One is, for truly small businesses, you may want to think about some limitation or some exemption. The FTC report that I referenced from 2012, talks about data protection and privacy protections in the context of both

the transaction and the entity that is doing the collection. So, you would treat Amazon differently than you would treat a chain of local markets, for example, and that is one way you can do it. But I absolutely agree with you, and we want to work with this committee as you move forward with legislation, but I absolutely agree with you that you do not want privacy legislation to have anti-competitive effects. And that is critical as you move forward, and we have seen, it is early reports, but we have seen, as you pointed out, evidence of barriers to entry, and for new entrants in Europe as a result of GDPR.

Senator YOUNG. We will just go down the line because I cannot see your name tags. I am one degree removed from you.

Mr. BECKERMAN. Thank you, Senator. You are absolutely right, and this is a major consideration that we have to have. You do not want to create a regulatory mode over, you know, that protects incumbents, and need to come up with a standard that sets companies up of all sizes to be successful and provide the privacy and security that people want.

Mr. DODGE. Retail industry is one of the most competitive industries that exist. We thrive in competition. We believe it should exist everywhere. You need to take into consideration the impact on small businesses and breathing lots of innovation into the whole ecosystem.

Senator YOUNG. Any specific thoughts about how we might do that? I know it is a difficult question, but how we might tailor our standards to—

Mr. DODGE. I think it is acknowledging that some businesses are not a risk. Some businesses, the kind of information that they collect may not be of great risk. Looking at it that way, not just on size but on the types of data that they have. How much they transact in data.

Senator YOUNG. OK.

Ms. ESPINEL. I mean, obviously you do not want to create a situation where small companies can buy like privacy or creates some sort of perverse incentive to organize and collect and keep your data, and a governance structure that would allow people to take advantage of that. But it is also true that we do not want to harm innovation. We do not want to harm small businesses. So, I think it is something we should definitely be taking into account in terms of, you know, what we believe should be in strong Federal privacy legislation. I do not—we think that it would be well within the ability of small businesses to do so. We think we have crafted a proposal that would allow that, but it is an important issue and it is one that everyone should keep in mind.

Mr. ROTHENBERG. Senator, one answer to that is quite clearly to spell out, as we have been arguing, in a new paradigm series of activities that are prohibited and activities that are allowed. So, use of data for red lining or discrimination should be prohibited. Use of data to send dog food ads to dog owners or presumed dog owners is not very harmful. In fact, it is beneficial to them. We think that should be allowed.

Dr. HARTZOG. So, I would just note that I think that even—

Senator YOUNG. The dog food lobbyists would love to hear that. [Laughter.]

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

The CHAIRMAN. Thank you, Senator Young.

Senator YOUNG. Thank you.

The CHAIRMAN. Senator Cruz.

**STATEMENT OF HON. TED CRUZ,
U.S. SENATOR FROM TEXAS**

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

Mr. LEIBOWITZ. I would say it is a good idea. You were at the FTC when they did a pharmaceutical task force, and that resulted in enormous benefits for consumers and for competition. I think this is very, very similar and modeled on that effort. And I think they should—well, I will let the current FTC figure out what they want to do, but I think this is a great announcement and I think they should use all of the authority of their agency to see whether there any anti-competitive behavior in tech companies. I assume that is what they are doing.

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

Mr. BECKERMAN. I will jump in here Senator, if that is alright. When I look at the Internet and Internet platforms, I do see them as one of the greatest places for free speech and open expression anywhere.

In particular as you look to conservative voices. They have found an audience online and there are countless examples of individuals who may be would not have been picked up at a newspaper or even on a Fox News, who are able to build audience of millions and millions of people and become household names, and then later get picked up on TV programs because of the internet. And it does provide incredible opportunity for all Americans, and I do not necessarily think you would want to see the Government stepping in to regulate speech there.

Mr. LEIBOWITZ. Well I agree with that. And going back to the tech task force, you know, one of the other tools in the FTC's arse-

nal is of course the 6B study, which is the industry-wide study where it just brings to public life the way that an industry is focusing or the way it is operating. And I suppose one possibility is they are looking at a potential 6B.

Senator CRUZ. Well and let me amplify that because one of the most frustrating things about dealing with the question of tech censorship, it is that it is all marked in darkness and obscurity. There is no transparency whatsoever. Both this committee and the Judiciary Committee, on which I also sit, have repeatedly asked tech companies, even basic barebones data in terms of how many speakers on their social media platform are they silencing, to what extent are they engaging in shadow banning. And shadow banning by its nature has been reported to be a process where a particular speakers is silenced but that speaker does not know it because they send out a tweet, they sent out a post, they appear to be communicating, and yet the tech platform does not allow those, including those who have affirmatively opted-in and chosen to hear that speaker, simply does not allow them to hear that speaker. And those words, that speech, goes into the ether.

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

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

Mr. BECKERMAN. Senator, transparency is important and there always can be greater levels of transparency. I will say that these platforms seek to serve all Americans regardless of political views and are open platforms to do so.

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

Mr. BECKERMAN. Each platform has a different set of community standards that perhaps we could do a better job of making more clearer and more transparent in what they are, and certainly mistakes are made. Sometimes with voices on the right, but mistakes are often made with voices on the left.

Senator CRUZ. Can you give me an example?

Mr. BECKERMAN. Not off the top of my head, but I mean——

Senator CRUZ. Yes, nobody else can either. That is the lack of transparency right there. And one debates these issues using anecdotes. Anecdotes are not a very good way to debate an issue, but the reason you are forced to use anecdote is because there are no data, there is no evidence, there are no objective numbers, because of the lack of transparency. Thank you.

The CHAIRMAN. Thank you, Senator Cruz. Senator Cantwell has informed me that she has no follow-up questions and neither do I. So, the hearing record will remain open for two weeks. During this time, Senators are asked to submit any question for the record. Upon receipt, the witnesses are requested to submit their written answers to the Committee as soon as possible, but no later than Wednesday, March 13, 2019.

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

[Whereupon, at 12:15 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO
JON LEIBOWITZ

Question 1. The new California privacy law preempts cities like San Francisco and Los Angeles from adopting their own privacy requirements for companies. I guess the California legislature didn't want a patchwork of municipal-level privacy laws. How is that approach any different than Congress preempting a patchwork of state-level privacy laws?

Answer. It is not any different. The same logic applies—a single, national law that protects consumers consistently throughout the United States (regardless of whether they live, work, or happen to be accessing the Internet) is preferable to a patchwork of state and/or local privacy laws.

Question 2. I have heard from many interested parties that the FTC currently lacks the resources needed to effectively enforce consumer privacy under its current Section 5 authorities. As a member of the Senate Appropriations Subcommittee with jurisdiction over the FTC, I am particularly interested in understanding the resource needs of the agency based on its current authorities, particularly before providing additional authorities. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

Answer. The FTC is the Nation's premier privacy enforcement agency. The enactment of a new privacy law for which the FTC is the primary enforcement agency would necessitate increasing the resources provided to the FTC to enforce the new law. The FTC budget has remained flat since 2012, and the agency currently has fewer full-time employees than it did in 1980, when the United States contained 100 million fewer people. Recently, in response to a request from Representatives Pallone and Schakowsky, FTC Chairman Simons stated that the Commission has only 40 full-time employees dedicated to overseeing Internet privacy and data security.

Depending upon the new law's final details, these increased resources may be necessary:

- To undertake investigations regarding whether companies are complying with the new law.
- To conduct enforcement proceedings to determine whether to use the FTC's civil forfeiture authority to impose fines for violations, including for a company's first violation of the statute, and to implement and enforce such penalties.
- To promulgate rulemakings required by the new law.

To hold hearings or workshops to help companies develop best practices for compliance with the new law.

Question 3. The Government Accountability Office (GAO) recently published a report in January regarding additional Federal authorities that could enhance consumer protections based on their review of past FTC privacy enforcement actions and input from industry, advocacy groups, and academia. One of the suggestions from GAO to enhance Internet privacy oversight was authorizing the FTC to levy civil penalties for first-time violations of the FTC Act. Would your organization support a Federal privacy bill that provides the FTC civil penalty authority?

Answer. Yes, though Congress may want to consider including factors that would help the FTC determine the appropriate size of a fine for first-time violations.

Question 4. At its core, the 2012 FTC Privacy Framework is based upon providing consumers with notice regarding a company's privacy practices, giving consumers choice about how their personal information is collected, used and shared, and seeking consumers' consent based upon the sensitivity of their personal information. Does that type of model still make sense today?

Answer. Yes, the 2012 FTC Privacy Framework is a very useful model for U.S. privacy law designed to protect consumers while preserving the vibrancy of our Nation's Internet economy, which leads the world in technological innovation and enhancing consumer welfare.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO
JON LEIBOWITZ

Question 1. Mr. Leibowitz: We need to give consumers more control over how their data is used. What tools could we give the FTC to take a more proactive approach to protecting consumers, short of full APA rulemaking authority?

Answer. The FTC would benefit from (1) clearer statutory authority to protect consumer privacy; (2) civil penalty authority, including for a first violation; (3) targeted rulemaking authority to implement specific provisions of a new, comprehensive Federal privacy law; and (4) the funding resources necessary to implement the new law and conduct investigations and enforcement actions.

Question 2. Mr. Leibowitz: I introduced the BROWSER Act in 2017, while I was the Chairman of the subcommittee on Communications & Technology in the House. It was one of the first bipartisan privacy bills introduced in Congress. It has a significantly lighter touch GDPR or CCPA. As we work through privacy legislation in this Congress, one of my top concerns has been surrounding location information, which we classified as "sensitive" information and thus subject to increased protections. Many delivery or rideshare companies felt this constrained their ability to serve their customers. Do you think we would be well suited to delineate between location information essential to the operation of a service, versus location information collected for purposes not related to the essential elements of the service?

Answer. Precise geo-location information should only be used or collected subject to a consumer's opt-in consent, unless such information is necessary to undertake the *service* requested by the consumer, or for other operational purposes such as network management and security as well as identity verification.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO
MICHAEL BECKERMAN

Question 1. The new California privacy law preempts cities like San Francisco and Los Angeles from adopting their own privacy requirements for companies. I guess the California legislature didn't want a patchwork of municipal-level privacy laws. How is that approach any different than Congress preempting a patchwork of state-level privacy laws?

Answer. Internet Association and our member companies support a consistent, economy-wide Federal privacy framework as opposed to a patchwork of state-or municipal-level privacy laws. Strong preemption ensures consumers have a consistent experience within and across state lines and will avoid a confusion patchwork of state and municipal laws that could hinder continued American leadership in technology. Congress is the most deliberate body in the world, and it should set a standard that is worthy of preemption.

Question 2. At a hearing last year, a witness from Google noted that complying with Europe's GDPR cost the company "hundreds of person-years." We're used to asking how many "person hours" compliance costs, but it's striking that this GDPR compliance is better expressed in years. Similarly, Garmin recently testified at an FTC hearing that it invested "800 person-months" in GDPR compliance (or "66 person-years"). Garmin is about twelve percent the size of Google, but as a percentage of the "person-years" available to either company, the investment is enormous. What does it mean for small companies who don't have spare "person-years" or "person-months" to invest? In your opinion, how do investors in startups evaluate these compliance costs? Would a complicated and expensive Federal regime dampen startup investment? As we draft legislation, how do we ensure that compliance costs also go toward protecting privacy? For example, should we make legislation scalable and targeted to the risk presented by a given data processing activity?

Answer. Flexibility is key in any successful privacy legislation. To achieve maximum benefit for individuals and remain mindful of the impact on small-and medium-sized businesses (SMBs), IA believes that Federal privacy legislation must allow for flexibility in how the desired outcomes and goals are achieved. Flexibility—allowing for a performance standard rather than a design standard—will allow better privacy protections for individuals as technology evolves. Flexibility will stimulate innovation, including in privacy enhancing technologies. It also avoids im-

posing unnecessary burdens on small business through overly prescriptive rules which create costs and impediments for growing businesses without necessarily providing meaningful privacy protections. Beyond legislative text, the FTC's mission of educating individuals on their rights and protections under the law ought to be encouraged and appropriately resourced. For example, the FTC recently launched a campaign to educate organizations on their obligations and best practices with the *Cybersecurity for Small Businesses* campaign. Programs such as this can help Federal regulators address the complexity inherent in any Federal legislation applied across the economy.

Question 3. I have heard from many interested parties that the FTC currently lacks the resources needed to effectively enforce consumer privacy under its current Section 5 authorities. As a member of the Senate Appropriations Subcommittee with jurisdiction over the FTC, I am particularly interested in understanding the resource needs of the agency based on its current authorities, particularly before providing additional authorities. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

Answer. The FTC has the expertise and skills necessary to be a strong regulator for consumer privacy. The FTC's track record shows that it engages in meaningful and transparent enforcement processes that improve the business community's compliance with consumer protection laws. The FTC also supports compliance through educational efforts and resources for regulated companies. The small business community, in particular, benefits from FTC guidance on legal compliance. Consumers also benefit, directly and indirectly, from FTC efforts. Consumers benefit directly from FTC efforts to support and educate consumers. And they benefit indirectly through FTC actions that improve the level of compliance of a single company or an entire industry sector through education, guidance, and enforcement. This is a broad remit for the FTC with its current scope of authority. There is no doubt that the FTC could do more with additional personnel and funding. IA supports increased resources for the FTC to continue its good work in all of these areas.

IA members support comprehensive Federal privacy legislation with the FTC as the lead regulator. A comprehensive Federal privacy bill would apply to all parts of the economy, across sectors, both online and brick-and-mortar companies. If such legislation is able to become law, it expands the number of actors who are subject to FTC regulation, poses new issues for enforcement, creates new potential violations, and potentially creates rulemaking needs to flesh-out application of the new law. IA supports the FTC receiving appropriate funding to enable the FTC to adopt a multi-pronged approach to enforcement, as it currently does under laws that exist today.

Question 4. The Government Accountability Office (GAO) recently published a report in January regarding additional Federal authorities that could enhance consumer protections based on their review of past FTC privacy enforcement actions and input from industry, advocacy groups, and academia. One of the suggestions from GAO to enhance Internet privacy oversight was authorizing the FTC to levy civil penalties for first-time violations of the FTC Act. Would your organization support a Federal privacy bill that provides the FTC civil penalty authority?

Answer. IA members believe that the FTC should have a range of authorities available to enforce Federal privacy legislation. In fact, the FTC has tools available in addition to civil fines and more tools could be added through the legislative process. For example, in the consumer protection context, the FTC can issue cease and desist notices, seek injunctions, sue for consumer redress, require reporting, and impose other accountability measures through consent decrees. The FTC should choose enforcement mechanisms that promote changes in behavior that bring companies into compliance with legal requirements and that are proportional with the grievousness of the harm to consumers and with the level of intent associated with non-compliance.

Even the best drafted privacy laws will not be able to anticipate every scenario, and companies acting in good faith could be found to have violated the law, despite their efforts to comply. In such situations, the appropriate and proportional remedy may not be a civil fine. The current system for FTC enforcement allows the FTC to seek to rectify violations in the first instance, and on the second occurrence impose fines. In general, this seems to allow the FTC to take the harshest action against the worst actors (those who violate consent decrees). If Congress concludes that the FTC should be more readily able to impose civil penalties, IA thinks that it would be worthwhile to provide an opportunity for the alleged violator to "cure" the violation before imposing penalties.

Question 5. The GDPR included a “data portability” requirement that allows consumers to request and receive their personal information from companies in a structured, commonly used and machine-readable format that can be imported by competing companies and services. Based on the experiences of your member companies, would someone please explain what compliance and enforcement with this requirement looks like? Please describe the consumer benefit of this requirement. 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. IA member companies support giving consumers a right to portability. This right of portability should allow consumers to obtain personal information that they provided to a service in a commonly used electronic format, so that the consumer is able to access their information without special tools. In addition, by using a commonly available file format it allows a consumer to transfer the content to another service. IA members believe that companies should not hinder the consumer’s ability to take their personal information to another service provider.

If a consumer uses a specific service to store photos electronically and they decide to change services—perhaps a new service offers more storage space for free—the consumer would be able to obtain the photos that the consumer provided to the original storage service in an electronic format. The consumer could then choose to upload that data to another service provider. This allows consumers to avoid being “locked in” to using specific services and can enhance competition.

Practically speaking, the value proposition is not as clear for every use case that could exist under a broad new privacy bill. In some contexts, companies may have valid concerns that providing consumers with broad access to data for portability could potentially expose their proprietary technology to competitors. IA purposely limits the obligation on the company to providing the consumer with an electronic copy of the personal information the consumer provided upon receiving a verified request. The company should select a format for disclosing the information that is machine-readable and commonly in use. This is where the company obligation would end. This helps limit burden on small businesses and makes the obligation more appropriate for the wide range of services that could be subject to a Federal privacy bill.

However, within sectors, particularly those where this type of consumer right makes the most sense, voluntary cooperation can promote portability. Companies may voluntarily choose to participate in efforts to develop a common framework to allow portability to work more seamlessly. For example, several IA members are working together on the Data Transfer Project, which would allow consumer information to be transferred directly from one company to another at the consumer’s request. In addition to industry efforts to promote standardization and cooperation to enhance the value of portability, the National Institute of Standards and Technology would be well placed to develop frameworks.

Question 6. At its core, the 2012 FTC Privacy Framework is based upon providing consumers with notice regarding a company’s privacy practices, giving consumers choice about how their personal information is collected, used and shared, and seeking consumers’ consent based upon the sensitivity of their personal information. Does that type of model still make sense today?

Answer. IA absolutely supports transparency and the right of consumers to be informed about the collection, use, and disclosure of their personal information. A publicly available privacy statement that contains a full accounting of privacy practices should be required by a Federal privacy law. However, privacy protection should not be dependent on a consumer’s review and understanding of a privacy statement. The notice and consent framework needs to be updated based on shared learnings about the model’s flaws. IA proposes that Congress adopt a framework that is less reliant on notice and choice, so that when a consumer is presented a notice and a choice it will be an infrequent event that a consumer will pay attention to and be able to make an informed choice.

Federal privacy legislation should establish a set of uses of personal information that companies may engage in without consumer consent. This list of practices should focus on uses that are consistent with consumer expectations based on their relationship with the company processing their information. For example, a consumer would not need to consent to have an e-commerce company disclose the delivery address for a purchase to the delivery company. The 2012 FTC Report also recognized that certain activities are consistent with consumer expectations and the consumer consent process does not provide any additional meaningful privacy protections. Likewise, the GDPR allows companies to process personal information for “legitimate interests” without obtaining user consent.

Within these generally recognized categories of activities, IA does not believe that there is a need to distinguish between personal information and sensitive personal information. The key is that the uses being made of the personal information or sensitive personal information are uses that are consistent with consumer requests or expectations. Outside these generally recognized categories, the sensitivity of personal information is a factor that should be considered as part of a risk assessment of the overall context of the processing activity. Processing activities that create serious privacy risks for consumers may require opt-in consent.

Question 7. Your testimony highlighted concerns that the new California law actually undermines the “proliferation of responsible data practices” and makes consumer information less protected by discouraging privacy enhancing techniques like de-identification. Would you please explain to this committee how the California law fails in this sense?

Answer. IA companies support many of the privacy-enhancing concepts that motivated provisions of the CCPA, such as consumer rights to access, deletion, transparency, and choice. Notwithstanding IA’s support for these concepts, IA has significant concerns with how these were implemented in the actual statutory text of the CCPA. IA believes that Americans deserve better privacy protections than what CCPA provides.

A Federal privacy law should be more comprehensive in coverage, provide stronger user rights, and require more responsibility by entities that process personal information. For example, IA privacy principles call for user rights to access, correction, and deletion. CCPA only allows access and deletion, not correction. CCPA does not require any consumer consent for processing personal information of adults, even where such processing may present serious privacy risks to the consumer. Additionally, CCPA puts consumer information at risk by allowing disclosure of personal information to any member of a “household” or to any user of a shared device.

The California law does not encourage the use of industry best practices due to a lack of clarity around deidentified, aggregate, and pseudonymous data. These practices allow companies to divorce personally identifying information from data, making information more secure and less likely to cause harm in the unfortunate instance of a data breach. The construction of the CCPA demonstrates a clear legislative intent to exempt “deidentified” data, but poorly constructed provisions create confusion. There are multiple places in the statutory text of the CCPA that information that is not linked to particular consumers should not be treated as personal information. First, “deidentified” is defined in such a way that it is the direct opposite of “personal information.” Personal information is defined as simply the opposite of information “that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” Thus, information that complies with the requirements of the definition of deidentified, should not be viewed as “personal information” for the purposes of the CCPA. The CCPA goes further to underscore that the obligations of the statute do not apply to information that is not personally identifiable. The exemptions in Civil Code section 1798.145, subdivision (a) state that “the obligations imposed on businesses by this title shall not restrict a business’s ability to” “collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.” The Legislature repeated in section 1798.145, subdivision (i) that a business is not “require[d] to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.” In addition to these broad exemptions, section 1798.100, subdivision (e) states that a business is not required to “reidentify or otherwise link information that is not maintained in a manner that would be considered personal information” to comply with a consumer request for access. This exact language is repeated in section 1798.110, subdivision (d)(2) pertaining to consumer deletion requests.

IA member companies support the laudable goal of encouraging companies to use privacy enhancing techniques to minimize the amount of personal information collected, processed, stored, and disclosed about consumers. The CCPA should reduce the risk to consumers from potential inadvertent disclosure, unauthorized acquisition, and from unnecessary privacy intrusions. In addition, it should ensure that businesses are not forced to link or combine data in such a way that it creates “personal information” solely to enable compliance with a consumer request under CCPA. As is clear from the above provisions, the CCPA did not intend for businesses to take steps to combine information and make more information identifiable than is done in the normal course of business. References that are not in parallel construction with this “linkable” standard should not jeopardize the operation of these sections. For example, the language in Civil Code section 1798.130, subdivision (a)(3)(A) which says, “associate the information provided by the consumer” should be read in a manner consistent with the carve-outs for non-personally identi-

fiable information, and should not force businesses to engage in the linking or association of data not otherwise linked or associated by the business with a consumer.

Furthermore, a fractured approach to privacy harms consumers. We see states across the country eager to follow in California's footsteps working on state privacy laws, some of which will resemble CCPA and others of which will adopt a dramatically different approach. For companies that currently operate globally and are subject to GDPR, conflicts already exist. For example, CCPA's requirements to allow consumer access to information about a "household" could force a company to violate the privacy protections of the GDPR by disclosing information collected while an EU resident visited friends in California and used the "household" wifi network.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CORY GARDNER TO
MICHAEL BECKERMAN

Question 1. Mr. Beckerman, news reports have indicated that a number of companies have installed microphones or cameras into internet-connected devices that were not previously disclosed to consumers or users of those devices. I understand that sometimes companies want to prepare their devices for future updates and those microphones or cameras may not even be intended to be operable until a later date. But I still strongly believe that companies should always disclose to consumers when devices include such sensitive technology. Do you believe that companies selling Internet connected devices should always disclose to consumers when those devices have microphones or cameras embedded in them—even if that microphone or camera was installed without nefarious intent?

Answer. 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.

The commitment to transparent data practices should apply across different means of collecting personal information from consumers. Where a technology is not currently being used to collect personal information, it would be appropriate for companies to assess the privacy risk to the consumer of including specific technology in a product. A risk assessment may take into account the level of functionality of the technology included in the product and any privacy protections for consumers in the event of unauthorized access and use of the technology. If privacy risk is not appropriately mitigated, consumers should be notified of the technology in the product.

Question 2. Mr. Beckerman, I've spoken at this Committee before about my belief that American companies should tread carefully when operating in countries with horrific track records on human rights. The privacy of targeted minority groups like the Uyghurs in China or the Rohingya in Myanmar is enormously important and often a matter of life and death. There is a careful balance to achieve between seeking new markets and bringing communications services and platforms to people around the globe and ensuring that those new services do not further the antidemocratic, discriminatory, and sometimes murderous objectives of certain foreign actors. How are your member companies grappling with the question of safeguarding privacy on the global scale? What more can Congress be doing to further those efforts?

Answer. IA member companies appreciate your continued efforts to advocate for human rights around the world, particularly in the digital space, and believe that the United States Trade Representative (USTR) can do much to aid those efforts. In addition, IA believes that American leadership through Federal privacy legislation would aid companies in being able to apply American principles for privacy and free expression globally. IA member companies have also adopted privacy and security measures that benefit their users around the globe, including privacy settings, encryption, two-factor authentication and other tools that give users more control and protection against breaches of their privacy.

IA submitted comments to USTR on the National Trade Estimate Report for 2019 in October 2018 that discussed the types of measures that oppressive regimes are adopting that either exclude companies from the local market or that would require compliance activities that run contrary to globally recognized human rights frameworks and proposed action that the U.S. government can take to respond.

The Internet ecosystem flourishes when users and content creators are empowered through an open architecture that promotes the unrestricted exchange of ideas and information. Internet services instantaneously connect users to goods and services, facilitate social interactions, and drive economic activity across borders. Consequently, support for the free flow of information is vital to eliminate trade barriers that restrict commerce or prevent U.S.-based Internet services the freedom to operate in a foreign jurisdiction. Unfortunately, data localization mandates and other limits on data transfers are increasingly restricting U.S. services from accessing overseas markets. While China and Russia have had data localization requirements in place, other countries are threatening to follow suit, particularly in the Asia-Pacific region. These and other foreign governments frequently cite concerns about security, privacy, and law enforcement access to justify localization measures. However, as the U.S. responds to these measures, it is critical to convey that data localization requirements typically increase data security risks and costs—as well as privacy risks—by requiring storage of data in a single centralized location that is more vulnerable to natural disaster, intrusion, and surveillance. In practice, the primary impact of a data localization measure is not to safeguard data but instead to wall off local markets from U.S. competition, while hurting local businesses as well.

To give users and companies greater assurance that privacy will be protected on a cross-border basis, IA urges USTR to ensure that privacy protections are implemented in an objective and non-discriminatory way. In addition, it is important to encourage mechanisms that promote compatibility between different privacy regimes, as opposed to unilateral regulations that do not provide a basis for transferring data on a cross-border basis.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARSHA BLACKBURN TO
MICHAEL BECKERMAN

Question. Mr. Beckerman: Recently, Facebook announced “its pivot to privacy” plans. As part of this privacy shift, Facebook plans to integrate its three messaging platforms—Whatsapp, Instagram, and Messenger—and to add the encryption in Whatsapp to the other two messaging apps. But some experts predict that Facebook is actually moving in the direction of a popular service in China called WeChat. WeChat is an all-purpose app that allows you to do everything in one app, from making payments to ordering food to sharing pictures. If Facebook were to operate like WeChat, more and more consumer data would be shared across payments, messaging, and e-commerce. As the FTC wraps up its investigation into Facebook for data privacy violations, should there be greater concern about Facebook’s new plans to integrate its messaging platforms?

Answer. End-to-end encryption systems offer consumers substantial privacy protections, not only against government surveillance, privacy and security threats from bad actors, but also from the providers of the services that enable the end-to-end encrypted communications. Consumers benefit substantially from the privacy and security protections provided by an end-to-end encrypted channel. Congress and the FTC should guard against efforts to undermine the security protections provided by strong encryption and take a strong stand against requirements for back doors or built-in vulnerabilities as they can be exploited by bad actors.

To our knowledge, WeChat retains access to messages in an unencrypted form on WeChat’s servers (see *here*). This allows both government surveillance and provider access to the content of user messages. <https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?opcode=2&id=1208117b2mai1410243yyqfz&lang=en&plat=2&Channel=helpcenter>

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO
BRIAN DODGE

Question 1. The new California privacy law preempts cities like San Francisco and Los Angeles from adopting their own privacy requirements for companies. I guess the California legislature didn’t want a patchwork of municipal-level privacy laws. How is that approach any different than Congress preempting a patchwork of state-level privacy laws?

Answer. There is no difference. The rationale for a state law that prevents a patchwork of municipal-level privacy laws is perfectly consistent with the rationale of a Federal law that preempts states. This unique moment requires private sector leadership and retailers are prepared for the responsibility to lead the effort to craft an American privacy framework that balances the need to protect consumers and foster the dynamic market innovation that our country is built upon. A pragmatic

national privacy framework will provide clear and consistent outcomes that meet the needs of consumers and businesses. Strong Federal preemption is necessary to prevent a balkanized regulatory landscape and bring uniformity and rationality to myriad potential approaches.

Question 2. I have heard from many interested parties that the FTC currently lacks the resources needed to effectively enforce consumer privacy under its current Section 5 authorities. As a member of the Senate Appropriations Subcommittee with jurisdiction over the FTC, I am particularly interested in understanding the resource needs of the agency based on its current authorities, particularly before providing additional authorities. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

Answer. RILA does not have specific resource-based recommendations and defers to the Committee to determine the appropriate amounts. As a general matter, RILA does support additional Federal funding and personnel at the FTC particularly to address the expanded enforcement requirements that would flow from a comprehensive Federal privacy law.

Question 3. The Government Accountability Office (GAO) recently published a report in January regarding additional Federal authorities that could enhance consumer protections based on their review of past FTC privacy enforcement actions and input from industry, advocacy groups, and academia. One of the suggestions from GAO to enhance Internet privacy oversight was authorizing the FTC to levy civil penalties for first-time violations of the FTC Act. Would your organization support a Federal privacy bill that provides the FTC civil penalty authority?

Answer. RILA has supported “first to fine” language in our efforts to solve the data breach issue and supports providing the FTC such authority as part of a comprehensive preemptive Federal privacy law.

Question 4. 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. Based on the experiences of your member companies, would someone please explain what compliance and enforcement with this requirement looks like? Please describe the consumer benefit of this requirement. 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. Retailers believe further scrutiny by policymakers is required to determine how best to implement this concept in the US. This is an important concept which can, for example, enhance competition in the social media space, but in other industries porting certain user generated data may ultimately create anticompetitive outcomes. To avoid these unintended consequences, retailers believe that protecting proprietary business methods requires limiting portable data to content generated and submitted by the user, which would exclude data such as inferences drawn by the organization about the user or other data generated by the organization. Additionally, in order to prevent dominant market participants from unfairly incentivizing other organizations’ consumers to exercise a right of portability, the data portability right should be limited to user-generated content that has a significant creative component, such as photographs, original prose, etc.

Question 5. At its core, the 2012 FTC Privacy Framework is based upon providing consumers with notice regarding a company’s privacy practices, giving consumers choice about how their personal information is collected, used and shared, and seeking consumers’ consent based upon the sensitivity of their personal information. Does that type of model still make sense today?

Answer. Leading retailers believe in respecting customers’ wishes by providing reasonable control over their personal information. But, too often this debate descends into the binary options of mandatory consent for every use on the one hand and no consent for any use on the other. The 2012 FTC Privacy Framework does have value, but it is incomplete. Retailers support providing control, access, correction, and deletion rights including allowing consumers to limit sharing data with third-parties like advertisers and restrictions on targeted advertising. Retailers believe which controls to offer, when to offer them, and how they are offered should depend on context. For example, a transaction that includes delivery necessarily includes the transmission of a customer’s address to the third-party delivery service. The context of this transaction should not require consent because transferring address information is necessary to meet the customer’s desire for delivery.

Context may also include a variety of legal, technical, financial, and security requirements that must be correctly weighed. For example, a retailer may need to re-

tain consumer information when it is needed to secure a transaction, prevent fraud, or comply with the law. In addition, retailers believe that policymakers should carefully evaluate the implications of multichannel collection environments by recognizing that all collection is not electronic through easily consolidated data systems but may include a variety of interactions such as one to one connections through store associates and service professionals. A privacy approach that evaluates data use in context better addresses the business models and uses of data in the marketplace today rather than relying on foundational consent models alone.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO
RANDALL ROTHENBERG

Question 1. The new California privacy law preempts cities like San Francisco and Los Angeles from adopting their own privacy requirements for companies. I guess the California legislature didn't want a patchwork of municipal-level privacy laws. How is that approach any different than Congress preempting a patchwork of state-level privacy laws?

Answer. IAB believes that in the same way the California Consumer Protection Act preempts all rules, regulations, codes, ordinances, and other consumer privacy laws adopted by a city, county, or municipality, so too should a Federal privacy standard preempt such state laws.

IAB strongly encourages this Federal preemptive privacy standard for several reasons. For one, a patchwork of city or state privacy laws will create consumer confusion, since consumers expect baseline protections regardless of the city or state they happen to be in at any given time. Americans deserve consistent, privacy protective laws regardless which town, city, or state they are located.

Secondly, a patchwork of hundreds or thousands of city and 50 state privacy laws presents significant challenges for businesses trying to comply with these laws. This is particularly true for smaller businesses that lack the resources necessary to comply with a complex patchwork of regulations.

Ultimately, a patchwork of local privacy laws, especially in the context of the border-less internet, will fall short of consumers' expectations about their digital privacy.

Question 2. I have heard from many interested parties that the FTC currently lacks the resources needed to effectively enforce consumer privacy under its current Section 5 authorities. As a member of the Senate Appropriations Subcommittee with jurisdiction over the FTC, I am particularly interested in understanding the resource needs of the agency based on its current authorities, particularly before providing additional authorities. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

Question 3. The Government Accountability Office (GAO) recently published a report in January regarding additional Federal authorities that could enhance consumer protections based on their review of past FTC privacy enforcement actions and input from industry, advocacy groups, and academia. One of the suggestions from GAO to enhance Internet privacy oversight was authorizing the FTC to levy civil penalties for first-time violations of the FTC Act. Would your organization support a Federal privacy bill that provides the FTC civil penalty authority?

Answers to 2 and 3. We believe that for privacy laws to be effective, they require strong and meaningful enforcement tools by regulators. To date, the FTC has been a global leader in bringing privacy enforcement cases and shaping a privacy and data security framework, and we recognize that a new law may necessitate additional resources to ensure the FTC has the tools that it needs.

IAB supports legislative frameworks that strengthen privacy oversight and enforcement in order to enhance the FTC's longstanding expertise in overseeing privacy issues. To that end, we believe a new privacy law should consider 1) providing the FTC with additional privacy staff and resources, 2) granting privacy jurisdiction over common carriers and nonprofits, 3) granting strengthened and specific rule-making authority to the FTC; and 4) authorizing strict penalties for companies that engage in prohibited privacy practices.

Question 4. At its core, the 2012 FTC Privacy Framework is based upon providing consumers with notice regarding a company's privacy practices, giving consumers choice about how their personal information is collected, used and shared, and seeking consumers' consent based upon the sensitivity of their personal information. Does that type of model still make sense today?

Answer. Notice and choice are important privacy concepts that, when used appropriately, can enhance consumer trust. Our commitment to notice and choice is exemplified through IAB's integral role in the creation of the Digital Advertising Alliance ("DAA"), an industry body convened a decade ago to create a self-regulatory code for all companies that collect or use data for interest-based advertising online.

The DAA principles provide consumer notice and transparency through the DAA's YourAdChoices Icon, which provides consumers with information about interest-based advertising outside of the privacy policy. The DAA's YourAdChoices Icon also provides control regarding data collection and use of web viewing data and application use data through a simple, one-button tool.

While IAB believes there is a role for notice and choice in a Federal privacy law, it is also true that a rigid notice and choice framework can impose significant burdens on consumers, such as rampant over-notification which can lead to consent fatigue and an indifference to important notices regarding consumers' privacy. For example, the consent banners mandated by GDPR have been notably ineffective at curbing irresponsible data practices or truly furthering consumer awareness and choice.

We believe the time is right for a new, Federal paradigm on consumer privacy that goes beyond notice and choice by establishing clear rules that describe which data practices are permitted and prohibited, and that distinguishes between data practices that pose a threat to consumers and those that do not.

