

PROTECTING CONSUMER PRIVACY IN THE ERA OF BIG DATA

HEARING BEFORE THE SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED SIXTEENTH CONGRESS FIRST SESSION

FEBRUARY 26, 2019

Serial No. 116–7



Printed for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

36–508 PDF

WASHINGTON : 2020

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois	GREG WALDEN, Oregon
ANNA G. ESHOO, California	<i>Ranking Member</i>
ELIOT L. ENGEL, New York	FRED UPTON, Michigan
DIANA DeGETTE, Colorado	JOHN SHIMKUS, Illinois
MIKE DOYLE, Pennsylvania	MICHAEL C. BURGESS, Texas
JAN SCHAKOWSKY, Illinois	STEVE SCALISE, Louisiana
G. K. BUTTERFIELD, North Carolina	ROBERT E. LATTA, Ohio
DORIS O. MATSUI, California	CATHY McMORRIS RODGERS, Washington
KATHY CASTOR, Florida	BRETT GUTHRIE, Kentucky
JOHN P. SARBANES, Maryland	PETE OLSON, Texas
JERRY McNERNEY, California	DAVID B. McKINLEY, West Virginia
PETER WELCH, Vermont	ADAM KINZINGER, Illinois
BEN RAY LUJAN, New Mexico	H. MORGAN GRIFFITH, Virginia
PAUL TONKO, New York	GUS M. BILIRAKIS, Florida
YVETTE D. CLARKE, New York, <i>Vice Chair</i>	BILL JOHNSON, Ohio
DAVID LOEBSACK, Iowa	BILLY LONG, Missouri
KURT SCHRADER, Oregon	LARRY BUCSHON, Indiana
JOSEPH P. KENNEDY III, Massachusetts	BILL FLORES, Texas
TONY CARDENAS, California	SUSAN W. BROOKS, Indiana
RAUL RUIZ, California	MARKWAYNE MULLIN, Oklahoma
SCOTT H. PETERS, California	RICHARD HUDSON, North Carolina
DEBBIE DINGELL, Michigan	TIM WALBERG, Michigan
MARC A. VEASEY, Texas	EARL L. "BUDDY" CARTER, Georgia
ANN M. KUSTER, New Hampshire	JEFF DUNCAN, South Carolina
ROBIN L. KELLY, Illinois	GREG GIANFORTE, Montana
NANETTE DIAZ BARRAGÁN, California	
A. DONALD McEACHIN, Virginia	
LISA BLUNT ROCHESTER, Delaware	
DARREN SOTO, Florida	
TOM O'HALLERAN, Arizona	

PROFESSIONAL STAFF

JEFFREY C. CARROLL, *Staff Director*
TIFFANY GUARASCIO, *Deputy Staff Director*
MIKE BLOOMQUIST, *Minority Staff Director*

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

JAN SCHAKOWSKY, Illinois
Chairwoman

KATHY CASTOR, Florida
MARC A. VEASEY, Texas
ROBIN L. KELLY, Illinois
TOM O'HALLERAN, Arizona
BEN RAY LUJAN, New Mexico
TONY CARDENAS, California, *Vice Chair*
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
BOBBY L. RUSH, Illinois
DORIS O. MATSUI, California
JERRY McNERNEY, California
DEBBIE DINGELL, Michigan
FRANK PALLONE, Jr., New Jersey (*ex officio*)

CATHY McMORRIS RODGERS, Washington
Ranking Member
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
LARRY BUCSHON, Indiana
RICHARD HUDSON, North Carolina
EARL L. "BUDDY" CARTER, Georgia
GREG GIANFORTE, Montana
GREG WALDEN, Oregon (*ex officio*)

C O N T E N T S

	Page
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement	3
Prepared statement	4
Hon. Cathy McMorris Rodgers, a Representative in Congress from the State of Washington, opening statement	5
Prepared statement	7
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	8
Prepared statement	10
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	11
Prepared statement	12
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, prepared statement	101

WITNESSES

Brandi Collins-Dexter, Senior Campaign Director, Color of Change	14
Prepared statement ¹	16
Answers to submitted questions	230
Roslyn Layton, Ph.D., Visiting Scholar, American Enterprise Institute	21
Prepared statement	23
Answers to submitted questions	232
Denise E. Zheng, Vice President, Technology and Innovation, Business Roundtable	34
Prepared statement	36
Answers to submitted questions	254
David F. Grimaldi, Jr., Executive Vice President, Public Policy, Interactive Advertising Bureau	39
Prepared statement	41
Answers to submitted questions	255
Nuala O'Connor, President and Chief Executive Officer, Center for Democracy & Technology	52
Prepared statement	54
Answers to submitted questions	258

SUBMITTED MATERIAL

Article of January 15, 2019, "2019 Data Privacy Wish List: Moving From Compliance To Concern," by Ameesh Divatia, Forbes.com, submitted by Mr. Luján	103
Statement of the Berkeley Media Studies Group, et al., "The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States," submitted by Ms. Schakowsky	105

¹ Ms. Collins-Dexter's entire statement, including supplemental material that does not appear in the printed edition, has been retained in committee files and also is available at <https://docs.house.gov/meetings/IF/IF17/20190226/108942/HHRG-116-IF17-Wstate-Collins-DexterB-20190226.pdf>.

	Page
Letter of February 26, 2019, from Brent Gardner, Chief Government Affairs Officer, Americans for Prosperity, to Ms. Schakowsky, submitted by Ms. Schakowsky	107
Letter of February 25, 2019, from Edward J. Black, President and Chief Executive Officer, Computer & Communications Industry Association, to Ms. Schakowsky and Mrs. Rodgers, submitted by Ms. Schakowsky	108
Letter of February 13, 2019, from Access Humboldt, et al., to U.S. Senator Roger Wicker, et al., submitted by Ms. Schakowsky	115
Letter of February 25, 2019, from American Hotel & Lodging Association, et al., to Mr. Pallone, et al., submitted by Ms. Schakowsky	119
Letter of February 25, 2019, from Gary Shapiro, President and Chief Executive Officer, Consumer Technology Association, to Mr. Pallone, et al., submitted by Ms. Schakowsky	122
Comments of November 9, 2018, submitted by Engine to the Department of Commerce, Docket Number 180821780–878–01, submitted by Ms. Schakowsky	124
Letter of February 25, 2019, from Evan Engstrom, Executive Director, Engine, to Ms. Schakowsky, et al., submitted by Ms. Schakowsky	134
Statement of the American Bankers Association, February 26, 2019, submitted by Ms. Schakowsky	135
Letter of February 26, 2019, from David French, Senior Vice President, Government Relations, National Retail Federation, to Mr. Pallone, et al., submitted by Ms. Schakowsky	144
Letter of November 9, 2018, from David French, Senior Vice President, Government Relations, National Retail Federation, to David J. Redl, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration, Department of Commerce, submitted by Ms. Schakowsky	152
Letter of February 26, 2019, from Scott Talbott, Senior Vice President of Government Affairs, Electronic Transactions Association, to Ms. Schakowsky and Mrs. Rodgers, submitted by Ms. Schakowsky	166
Letter of February 26, 2019, from Jon Leibowitz, Co-Chair, 21st Century Privacy Coalition, to Mr. Pallone, et al., submitted by Ms. Schakowsky	170
Letter of February 26, 2019, from Mark Neeb, Chief Executive Officer, Association of Credit and Collection Professionals, to Ms. Schakowsky and Mrs. Rodgers, submitted by Ms. Schakowsky	173
Letter of February 25, 2019, from Will Rinehart, Director of Technology and Innovation Policy, American Action Forum, to Ms. Schakowsky and Mrs. Rodgers, submitted by Mrs. Rodgers	175
Letter of February 25, 2019, from Thomas A. Schatz, President, Council for Citizens Against Government Waste, to Mr. Pallone, et al., submitted by Mrs. Rodgers	190
Letter of February 26, 2019, from the Coalition for a Secure and Transparent Internet to Ms. Schakowsky and Mrs. Rodgers, submitted by Mrs. Rodgers ..	193
Letter of February 26, 2019, from Charles Duan, Technology and Innovation Policy Director, R Street Institute, et al., to Ms. Schakowsky and Mrs. Rodgers, submitted by Mrs. Rodgers	195
Letter of February 25, 2019, from Tim Day, Senior Vice President, U.S. Chamber of Commerce, to Ms. Schakowsky and Mrs. Rodgers, submitted by Mrs. Rodgers	198
Letter of February 25, 2019, from Katie McAuliffe, Executive Director, Digital Liberty, to subcommittee members, submitted by Mrs. Rodgers	204
Letter of February 25, 2019, from Michael Beckerman, President and Chief Executive Officer, Internet Association, to Ms. Schakowsky and Mrs. Rodgers, submitted by Mrs. Rodgers	206
Excerpt from Report of the Attorney General's Cyber Digital Task Force, Department of Justice, submitted by Mr. Latta	212
Statement by Google, undated, submitted by Mrs. Rodgers	216
Letter of February 26, 2019, from Jimi Grande, Senior Vice President, Government Affairs, National Association of Mutual Insurance Companies, to Mr. Pallone, et al., submitted by Mrs. Rodgers	228

VII

Letter of February 26, 2019, from Rob Atkinson, President, Information Technology and Innovation Foundation, et al., to Mr. Pallone and Mr. Walden, submitted by Mrs. Rodgers²

Page

²The letter has been retained in committee files and also is available at <https://docs.house.gov/meetings/IF/IF17/20190226/108942/HHRG-116-IF17-20190226-SD024.pdf>.

PROTECTING CONSUMER PRIVACY IN THE ERA OF BIG DATA

TUESDAY, FEBRUARY 26, 2019

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CONSUMER PROTECTION AND
COMMERCE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:01 a.m., in the John D. Dingell Room 2123, Rayburn House Office Building, Hon. Jan Schakowsky (chair of the subcommittee) presiding.

Members present: Representatives Schakowsky, Castor, Veasey, Kelly, O'Halleran, Luján, Cárdenas, Blunt Rochester, Soto, Rush, Matsui, McNerney, Dingell, Pallone (ex officio), Rodgers (subcommittee ranking member), Upton, Burgess, Latta, Guthrie, Bucshon, Hudson, Carter, Gianforte, and Walden (ex officio).

Also present: Representatives Eshoo and Clarke.

Staff present: Jeffrey C. Carroll, Staff Director; Elizabeth Ertel, Office Manager; Evan Gilbert, Press Assistant; Lisa Goldman, Counsel; Waverly Gordon, Deputy Chief Counsel; Tiffany Guarascio, Deputy Staff Director; Alex Hoehn-Saric, Chief Counsel, Communications and Technology; Zach Kahan, Outreach and Member Service Coordinator; Dan Miller, Policy Analyst; Joe Orlando, Staff Assistant; Kaitlyn Peel, Digital Director; Tim Robinson, Chief Counsel; Chloe Rodriguez, Policy Analyst; Mike Bloomquist, Minority Staff Director; Adam Buckalew, Minority Director of Coalitions and Deputy Chief Counsel, Health; Jordan Davis, Minority Senior Advisor; Melissa Froelich, Minority Chief Counsel, Consumer Protection and Commerce; Peter Kielty, Minority General Counsel; Bijan Koohmaraie, Minority Counsel, Consumer Protection and Commerce; Ryan Long, Minority Deputy Staff Director; Brannon Rains, Minority Staff Assistant; and Greg Zerzan, Minority Counsel, Consumer Protection and Commerce.

Ms. SCHAKOWSKY. The Subcommittee on Consumer Protection and Commerce will now be called to order.

So I am going to begin with a few comments that are off the clock and then invite our ranking member to do the same. I am going to say good morning and thank you all for joining us today. And before we officially start the hearing, I would like to welcome you to the first Consumer Protection and Commerce Subcommittee of the 116th Congress.

Consumer protection has long been my passion and what first drew me to public life. I like to call our subcommittee the Nation's legislative helpline because we field consumer complaints. The sub-

committee's jurisdiction is vast in scope, ranging from the safety of cars to consumer product defects to consumer fraud, both online and offline.

In the past, when Democrats controlled the House, this subcommittee was responsible for making pools and children's products safer, increased the fuel efficiency of cars, and made sure that agencies aggressively protect consumers over corporate interests. Under my leadership this subcommittee will be extremely active and push companies and the administration to put consumers first.

I look forward to working with Ranking Member McMorris Rodgers. I believe there are so many issues on which we will be able to work together in a bipartisan way. I would also like to welcome several new Democratic Members, Representative Mark Veasey from Texas—let's see, where I am looking the wrong way, OK—and Robin Kelly from Illinois, my home State; Tom O'Halleran from Arizona; Lisa Blunt Rochester from Delaware; and Darren Soto from Florida, are all new to the Energy and Commerce Committee and they also were smart enough to pick this best subcommittee at a very exciting time.

I also welcome back many familiar faces and appreciate your continued commitment to consumer protection issues. And I would like to thank Tony Cárdenas for serving as my vice chair of the subcommittee and he will provide the subcommittee with invaluable leadership.

And, finally, I would like to recognize the return of my friend Debbie Dingell. Over the past 2 weeks we have mourned the passing of her husband, John Dingell, who was so important to this committee over the years and a friend to so many. Debbie has been a stalwart, but I know it has been a difficult time.

Debbie, you have all of our sympathy and support from the entire subcommittee. And with the indulgence of my ranking member, just to let Debbie say a few words.

Debbie?

Mrs. DINGELL. I just want to thank you and all of my colleagues. John Dingell loved this committee. He thought the work that they did was very important, and I hear him in my ear going, "Woman, get on," and hearing him in the ears of everybody, "Work together for the American people." Thank you.

Ms. SCHAKOWSKY. I have been reminded that Darren Soto's birthday is today? Oh, yesterday. OK, never mind.

OK. So Ranking Member McMorris Rodgers, would you like to take a couple of minutes to welcome your new Members as well?

Mrs. RODGERS. Thank you. Thank you, Madam Chair and to all the members of the committee. Welcome to the committee, and I too want to extend my heartfelt thoughts and prayers to Debbie and so appreciate her friendship, her leadership on this committee, and I would join in saying let's work together. As John Dingell would challenge us, let's work together for the American people. And it is great to have you back, Debbie.

To the new members of the committee, I would like to recognize some of the newest Members on our side of the aisle: Mr. Hudson from North Carolina—he will be here shortly—Mr. Carter from Georgia, Mr. Gianforte from Montana, and I also have the privilege

of having former chairmen on this side of the aisle, Bob Latta and Burgess as well as full committee chairmen on this subcommittee.

I look forward to working with you, Madam Chair, on putting consumers first while ensuring that we continue to celebrate the innovation and all that it has meant to the American way of life and improving our quality of life. As Americans we have led the world in technology and innovation, and I look forward to the many issues that are before this committee and working to find that bipartisan ground wherever possible. Thank you.

Ms. SCHAKOWSKY. Let's shake on that.

Mrs. RODGERS. All right.

Ms. SCHAKOWSKY. All right. So I yield myself 5 minutes now for an opening statement.

OPENING STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

And as I said earlier, our subcommittee is the Nation's legislative helpline, and our first hearing, "Protecting Consumer Privacy in the Era of Big Data," couldn't be more timely because the phone at the end of the helpline is definitely ringing off the hook.

According to a recent survey, over 80 percent of U.S. adults were not very confident in the security of personal information held by social media, retail, and travel and travel companies, and 67 percent wanted the government to act to protect them. There is good reason for consumer suspicion. Modern technology has made the collection, analysis, sharing, and the sale of data both easy and profitable.

Personal information is mined from Americans with little regard for the consequences. In the last week alone, we learned that Facebook exposed individual private health information and they thought was—that consumers thought was protected in closed groups, and collected—and Facebook also collected data from third-party app developers on issues as personal as women's menstrual cycle and cancer treatment. People seeking solace may instead find increased insurance rates as a result of the disclosure of that information.

But Facebook isn't alone. We have seen the data collection industry transform from a nascent industry most Americans haven't heard of to an economic powerhouse gobbling up every piece of consumer data it can both online and offline. While many companies claim to provide notice and choice to consumers, the truth is that they provide little reason for believing we are protected.

Who has the time to wade through the dozens of privacy policies that impact them? How many people think about being trapped through their phone or by the overhead light in the store? And often, the only choice that we have to avoid data collection is not to go to the store or to use the app. Reports of the abuse of personal information undoubtedly give Americans the creeps.

But this data isn't being collected to give you the creeps. It is being done to control markets and make a profit. Without a comprehensive, Federal privacy law the burden has fallen completely on consumers to protect themselves and this has to end. Without a doubt, there are legitimate and beneficial reasons for consumers to use personal—for companies to use personal information, but

data collection must come with responsibilities. There should be limits on the collection of consumers' data and on the use and sharing of their personal information.

My goal is to develop strong, sensible legislation that provides meaningful protection for consumers while promoting competitive markets and restoring America's faith in business and government. Rules alone though are not enough. We also need aggressive enforcement. Unfortunately, in recent years the Federal Trade Commission's enforcement action have done little to curb the worst behavior in data collection and data security.

Any legislation must give Federal regulators the tools to take effective action to protect consumers. It is important to equip regulators and enforcers with the tools and funding necessary to protect privacy, but it is also critical to make sure that requests for more tools and privacy are not used as a excuse for inaction. We must understand why the FTC hasn't used its existing suite of tools to the full extent such as section 5 authority to ban unfair methods of competition or its ability to enforce violators.

So I welcome our witnesses today to learn about how we should achieve these goals given the breadth of the issue. This will be the first of several hearings. Others will allow us to focus on specific issues of concern to the public.

[The prepared statement of Ms. Schakowsky follows:]

PREPARED STATEMENT OF HON. JAN SCHAKOWSKY

Good morning and thank you all for joining us today. Before we start the hearing, I'd like to welcome you to the first Consumer Protection and Commerce Subcommittee of the 116th Congress. Consumer protection is my passion, and what first drew me to public life. I like to call our subcommittee the Nation's legislative helpline, because we field consumer complaints.

The subcommittee's jurisdiction is vast in scope, ranging from the safety of cars to consumer product defects to consumer fraud—both online and offline. In the past when Democrats controlled the House, this subcommittee was responsible for making pools and children's products safer, increasing the fuel efficiency of cars, and made sure agencies aggressively protected consumers over corporate interests.

Under my leadership, this subcommittee will be extremely active and push companies and the administration to put consumers first.

I look forward to working with Ranking Member McMorris Rodgers. I believe there are many issues on which we will be able to work together.

As I said earlier, our subcommittee is the Nation's legislative helpline, and our first hearing, "Protecting Consumer Privacy in the Era of Big Data," couldn't be more timely because the phone at the helpline is ringing off the hook. According to a recent SAS survey, over 80 percent of U.S. adults were not very confident in the security of personal information held by social media, retail, and travel companies and 67 percent wanted the government to act to protect them.

There is good reason for consumers' suspicion. Modern technology has made the collection, analysis, sharing, and sale of data both easy and profitable. Personal information is mined from Americans with little regard for the consequences.

In the last week alone, we learned that Facebook exposed individuals' private health information they thought was protected in closed groups, and collected data from third-party app developers on issues as personal as women's menstrual cycles and cancer treatments. People seeking solace may instead find increased insurance rates as a result of the disclosure of that information.

But Facebook isn't alone. We have seen the data collection industry transform from a nascent industry most Americans haven't heard of to an economic powerhouse gobbling up every piece of consumer data it can—both online and offline.

While many companies claim to provide notice and choice to consumers, the truth is this provides little real protection. Who has the time to wade through the dozens of privacy policies that impact them daily? How many people think about being tracked through their phones or by the overhead lights in a store? And often the

only “choice” they have to avoid data collection is not to go to the store or use an app.

Reports of the abuse of personal information undoubtedly give Americans the creeps. But this data isn’t being collected to give you the creeps. It’s being done to control markets and make a profit.

Without a comprehensive Federal privacy law, the burden has fallen completely on consumers to protect themselves. This must end.

Without a doubt, there are legitimate and beneficial reasons for companies to use personal information, but data collection must come with responsibilities. There should be limits on the collection of consumers’ data and on the use and sharing of their personal information. My goal is to develop strong, sensible legislation that provides meaningful protections for consumers while promoting competitive markets and restoring Americans’ faith in business and government.

Rules alone are not enough. We also need aggressive enforcers. Unfortunately, in recent years, the Federal Trade Commission’s (FTC) enforcement actions have done little to curb the worst behavior in data collection and data security. Any legislation must give Federal regulators the tools to take effective action to protect consumers. It is important to equip regulators and enforcers with the tools and funding necessary to protect privacy, but it is also critical to make sure that requests for more tools and privacy are not used as an excuse for inaction. We must understand why the FTC hasn’t used its existing suite of tools to the fullest extent, such as its Section 5 authority to ban “unfair methods of competition” or its ability to enforce violations of consent decrees.

I welcome our witnesses today to learn how we should achieve these goals. Given the breadth of this issue, this will be the first of several hearings. Others will allow us to focus on specific issues of concern to the public.

At the same time, I want to work with my colleagues on both sides of the aisle on drafting privacy legislation. I have talked to a number of you about your priorities, and I want them to be reflected in what gets reported from this subcommittee.

I look forward to working with each of you on this important issue.

I now yield to Ranking Member Cathy McMorris Rogers for 5 minutes.

Ms. SCHAKOWSKY. So I look forward to working with all of you on both sides of the aisle, and I now yield to Ranking Member Cathy McMorris Rodgers for 5 minutes.

**OPENING STATEMENT OF HON. CATHY McMORRIS RODGERS,
A REPRESENTATIVE IN CONGRESS FROM THE STATE OF
WASHINGTON**

Mrs. RODGERS. Thank you, Madam Chair. I would like to thank you for organizing this first hearing of the Congress on privacy and security. It really builds on important work that was done in the past by Chairman Walden and Latta in the last Congress and then Chairman Upton and Burgess in the 114th Congress. I am hopeful that we can find a bipartisan path to move forward on a single American approach to privacy, one that is going to protect consumers and individual privacy, one that ensures that consumers continue to benefit from the amazing technology and innovation that has happened in recent years.

This morning I would like to lay out four principles as we approach this effort, one that supports free markets, consumer choice, innovation, and small businesses, the backbone of our economy. We often celebrate small businesses in America.

Principle number 1, one national standard. The Constitution was crafted around the concept that one national marketplace would make America stronger in certain areas. It also recognizes the importance of intellectual property rights, free expression, and the rights of “We the People” to be protected from the power of government.

The internet knows no borders. It has revolutionized our Nation's economy by seamlessly connecting businesses and people across the country. Online, a small business in Spokane, Washington can as easily reach customers in Illinois and New Jersey as in Eastern Washington. Distance is no longer a barrier. The internet economy is interstate commerce and subject to Federal jurisdiction.

There is a strong groundswell of support for a Federal privacy law that sets a national standard. Many recognize the burdens multiple State laws would create, but what would it mean for someone in Washington State who buys something online from a small business in Oregon to ship to their family in Idaho? This is a regulatory minefield that will force businesses to raise prices on their customers. Setting one national standard makes common sense and is the right approach to give people certainty.

Principle number 2, transparency and accountability. Companies must also be more transparent when explaining their practices. For example, we learned last week that Google included a microphone in their Nest device but failed to disclose it, and Facebook is collecting very personal health information from apps, the Chair mentioned that. Transparency is critical. When unfair or deceptive practices are identified, there should be enforcement and there should be consequences strong enough to improve behavior.

Principle number 3, improving data security. Another area important to this debate is data security. Perfect security doesn't exist online, and companies are bombarded by hackers every second of every day. Certain data is more valuable on the black market, which is why Social Security Numbers, credit card data, and log-in credentials are always major targets for criminals. One goal must be to improve people's awareness. For one, how their information is being collected and used, and two, how companies are protecting it and how people can protect themselves.

Our focus should be on incentivizing innovation security solutions and certainty for companies who take reasonable steps to protect data, otherwise we risk prescriptive regulations that cannot be updated to keep up with the bad actors' newest tactics.

Principle number 4, small businesses. We must not lose sight of small- and medium-sized businesses and how heavy-handed laws and regulations can hurt them. Established, bigger companies can navigate a complex and burdensome privacy regime, but millions of dollars in compliance costs aren't doable for startups and small businesses. We have already seen this in Europe, where GDPR has actually increased, has helped increase the market share of the largest tech companies while forcing smaller companies offline with millions of dollars in compliance costs.

These startups and small businesses could be innovating the next major breakthrough in self-driving technology, health care, customer service, and so many other areas. To keep America as the world's leading innovator we cannot afford to hold them back. Heavy-handed and overly cautious regulations for all data will stop innovation that makes our roads safer, health care more accessible, and customer service experiences better.

I am glad our teams were able to work together on today's hearing. This is a good step forward in finding a bipartisan solution for these critical issues. And as we move forward, I am sure there is

going to be more hearings in the future to allow more small business owners, startups, and entrepreneurs to join this conversation.

I believe we have a unique opportunity here for a bipartisan solution that sets clear rules for the road on data privacy. In its best use data has made it possible for grocery aisles to be organized on how people shop. But we need to explore data privacy and security with forward-looking solutions, and I look forward to hearing from the witnesses and being a part of this discussion today.

Thank you very much, Madam Chair.

[The prepared statement of Mrs. Rodgers follows:]

PREPARED STATEMENT OF HON. CATHY McMORRIS RODGERS

Good morning and welcome to our first Consumer Protection and Commerce Subcommittee hearing. I would like to congratulate Chair Schakowsky.

I would also like to recognize the newest Members of the Subcommittee, Mr. Hudson from North Carolina, Mr. Carter from Georgia, and Mr. Gianforte from Montana. I look forward to working with all of the Members this Congress. Our jurisdiction includes vast portions of the economy and I look forward to working with you on bipartisan solutions that improve the lives of all Americans. I also would like to thank the Chair for organizing this first hearing of the Congress on privacy and security. This hearing builds on the good work of Chairmen Walden and Latta in the last Congress, and Chairmen Upton and Burgess in the 114th Congress. While there have been issues achieving bipartisan consensus in the past, I'm encouraged that we can find a bipartisan path forward on a single American approach to privacy—one that supports free markets, consumer choice, innovation and small businesses—the backbone of our economy.

Principle #1: One National Standard

The Constitution was crafted around the concept that one national marketplace would make America stronger in certain areas. It also recognizes the importance of intellectual property rights, free expression, and the rights of “We, the People” to be protected from the power of the government. The Internet knows no borders. It has revolutionized our nation's economy by seamlessly connecting businesses and people across the country.

Online, a small business in Spokane can just as easily reach customers in Illinois and New Jersey. Distance is no longer a barrier. The Internet economy is interstate commerce and subject to Federal jurisdiction. There is a strong groundswell of support for a Federal privacy law that sets a national standard. Many recognize the burdens a patchwork of State laws would create. What would it mean for someone in Washington State who buys something online from a small business in Oregon to ship to their family in Idaho? This is a regulatory minefield that will force businesses to raise prices on their customers. Setting one national standard is common sense and it's the right approach to give people certainty.

Principle #2: Transparency and Accountability

Companies must also be more transparent when explaining their practices. For example, we learned last week that Google included a microphone in their Nest device but failed to disclose it and Facebook is collecting very personal health information from apps. Transparency is critical. When unfair or deceptive practices are identified there should be enforcement and there should be consequences strong enough to improve behavior.

Principle #3: Improving Data Security

Another area important to this debate is data security. Perfect security doesn't exist online, and companies are bombarded by hackers every second of every day. Certain data is more valuable on the black market, which is why social security numbers, credit card data, and login credentials are always major targets for criminals. Our goal must be to improve people's awareness for one, how their information is being collected and used; two, how companies are protecting it; and three, how people can protect it themselves.

Our focus should be on incentivizing innovative security solutions and certainty for companies who take reasonable steps to protect data. Otherwise, we risk prescriptive regulations that cannot be updated to keep up with the bad actors' newest tactics.

Principle #4: Small Businesses

Finally, we must not lose sight of small and medium-sized businesses and how heavy-handed laws and regulations can hurt them. Established bigger companies

can navigate a complex and burdensome privacy regime. But millions of dollars in compliance costs aren't doable for startups and small businesses. We have already seen this in Europe, where GDPR has actually helped increase the market shares of the largest tech companies while forcing smaller companies offline with millions of dollars in compliance costs.

These startups and small businesses could be innovating the next major breakthrough in self-driving technology, health care, customer service, and more. To keep America as the world's leading innovator, we cannot afford to hold them back.

Heavy-handed and overly cautious regulations for all data will stop innovation that makes our roads safer, health care more accessible, and customer service experiences better. I'm glad our teams were able to work together on today's hearing. This is a good step forward to finding a bipartisan solution for these critical issues. As we move forward, I hope we make sure there's enough time before the next hearings to allow small business owners, startups, and entrepreneurs to join the conversation.

We have a unique opportunity here for a bipartisan solution that sets clear rules for the road on data privacy in America. In its best use, data has made it possible for grocery store aisles to be organized based on how people shop. By exchanging our data with email providers, we receive free email and photo storage. Ridesharing services analyze traffic patterns and real time data on accidents to get us home safer and faster. These are just some examples of how data in aggregate has saved us time and money, kept us safe, and improved our lives.

As we continue to explore data privacy and security, we must find a forward-thinking solution that fosters innovation and protects consumers from bad data practices that have caused people harm or create real risks. By achieving both, America will maintain our robust internet economy and continue to be the best place in the world to innovate.

Thank you again to all of the witnesses for being here today and I look forward to your testimony. I yield back.

Ms. SCHAKOWSKY. Thank you. The gentlelady yields back and now the Chair recognizes Mr. Pallone, chairman of the full committee, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you. I also wanted to welcome back Debbie Dingell. Debbie has shown tremendous strength and courage during the past few weeks, and you were missed, Debbie, and we are glad you are back today. So I just wanted to say that.

Welcome to the first hearing of the Consumer Protection and Commerce Subcommittee. We renamed the subcommittee to emphasize the importance of putting consumers first, and that is the lens through which I view the important issue of consumer privacy. How do we empower consumers and impose reasonable limits on companies that collect and use our own personal information?

In the past we have talked about major data breaches and scandals involving the misuse and unauthorized sharing of people's data and we have talked about the potential for emerging technologies to be used in unintended and potentially harmful ways. But privacy isn't just about major incidents or predictions of the future, it is an everyday issue constantly affecting our lives and the lives of our children.

Almost every company that we interact with and even many we don't are conducting surveillance of us. When we visit a single website, many companies are tracking our actions on that site, what we click on, how long we are on each page, even our mouse movements and that is true for each of the dozens of sites most of us visit every day.

When we go out our location is tracked on our phones. Video surveillance of stores, on the street, in doctors' offices record what we do and who we are with. The purchases we make are recorded by the stores through store loyalty programs and by the credit cards we use to make those purchases. And companies use that information to sort and commodify us too.

Inferences are drawn and we are labeled as a Democrat or Republican, white or Latino, gay or straight, pregnant teen, a grieving parent, a cancer survivor, so many more, and this is all done without our knowledge. And then our personal information and related inferences are being shared and sold many times over. Companies may share our information with business partners and affiliates that we have never heard of. Our data also may be sold to data brokers who collect massive amounts of data about all of us and then sell that off to anyone who is willing to pay for it.

The scope of it all is really mind-boggling. Without a doubt there are positive uses of data. Companies need personal information to deliver a package or charge for a service. Some data is used for research and development of new products and improving services and sometimes it is used for fraud prevention or cybersecurity purposes and some of it is used for scientific research to find new treatments for medical conditions.

But in some cases data use results in discrimination, differential pricing, and even physical harm. Low-income consumers may get charged more for products online because they live far away from competitive retailers. Health insurance companies could charge higher rates based on your food purchases or info from your fitness trackers. A victim of domestic violence may even have a real-time location tracking information sold to their attacker. And these are simply unacceptable uses of people's data.

Yet for the most part, here in the U.S. no rules apply to how companies collect and use our information. Many companies draft privacy policies that provide few protections and are often unread. One study calculated that it would take 76 years to read all the privacy policies for every website the average consumer visits every year.

And even if you could read and understand these privacy policies, often your only choice is to accept the terms or not use the service. In a lot of situations that is not an option. Consider when you need to pay for parking at a meter or use a website for work. You don't really have that choice. So we can no longer rely on a notice and consent system built on unrealistic and unfair foundations. As the chairwoman said, we need to look forward towards comprehensive privacy legislation, legislation that shifts the burden off consumers and puts reasonable responsibility on those profiting from the collection and use of our data.

Because consumer privacy isn't new to this committee, we have been talking about it for years, yet nothing has been done to address the problem and this hearing is the beginning of a long overdue conversation. It is time that we move past the old model that protects the companies using the data and not the people. So I look forward to hearing from our witnesses today on how we can work together to accomplish this. I plan to work with my colleagues on

both sides of the aisle to craft strong, comprehensive privacy legislation that puts consumers first.

And I just want to thank you, Chairman Schakowsky, when you said that, you know, what this committee is all about is putting consumers first, and I think that having this hearing as you are today on the privacy issue is a strong indication that that is exactly what we intend to do. Thank you again.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Welcome to the first hearing of the Consumer Protection and Commerce Subcommittee. We renamed the subcommittee to emphasize the importance of putting consumers first. And that is the lens through which I view the important issue of consumer privacy—how do we empower consumers and impose reasonable limits on companies that collect and use our personal information?

In the past, we've talked about major data breaches and scandals involving the misuse and unauthorized sharing of people's data. And we've talked about the potential for emerging technologies to be used in unintended and potentially harmful ways. But privacy isn't just about major incidents or predictions of the future. It's an everyday issue, constantly affecting our lives and the lives of our children.

Almost every company that we interact with, and even many we don't, are conducting surveillance of us. When we visit a single website, many companies are tracking our actions on that site—what we click on, how long we are on each page, even our mouse movements. And that's true for each of the dozens of sites most of us visit every day.

When we go out, our location is tracked on our phones. Video surveillance at stores, on the street, and in doctors' offices record what we do and who we are with. The purchases we make are recorded by the stores we buy from, through store loyalty programs, and by the credit cards we use to make those purchases.

Companies use that information to sort and commodify us, too. Inferences are drawn and we are labelled as gay or straight, Democrat or Republican, white or Latino, a pregnant teen, a grieving parent, a cancer survivor, and so much more. All without our knowledge.

Plus, our personal information and related inferences are being shared and sold many times over. Companies may share our information with business partners and affiliates, which may be strangers to you. Our data also may be sold to data brokers, who collect massive amounts of data about all of us, and then sell that off to anyone willing to pay for it. The scope of it all is mindboggling.

Without a doubt, there are positive uses of data. Companies need personal information to deliver a package or charge for a service. Some data is used for research and development of new products and improving services. Sometimes it's used for fraud prevention or cybersecurity purposes. And some is used for scientific research to find new treatments for medical conditions.

But in some cases, data use results in discrimination, differential pricing, and even physical harm. Low-income consumers may get charged more for products online because they live far away from competitive retailers. Health insurance companies could charge higher rates based on your food purchases or information from your fitness tracker. A victim of domestic violence may even have real-time location tracking information sold to their attacker.

Yet, for the most part, in the U.S., no rules apply to how companies collect and use our information. Many companies draft privacy policies that provide few protections and are often unread. One study calculated that it would take 76 years to read all of the privacy policies for every website the average consumer visits each year. And even if you could read and understand each privacy policy, often your only choice is to accept the terms or not use the service. And when you need to pay for parking at a meter or use a website for work, you don't really have that choice at all. We can no longer rely on a "notice and consent" system built on such unrealistic and unfair foundations.

As Chair Schakowsky said, we need to look toward comprehensive privacy legislation—legislation that shifts the burdens off consumers and puts reasonable responsibility on those profiting from the collection and use of our data.

As I said, consumer privacy isn't new to this committee. We've been talking about it for years. And yet, nothing has been done to address the problems. But times have changed. We are not going to fail consumers any more.

This hearing is beginning of that conversation. We need to move past the old model that protects the companies using the data, not the people. I look forward to hearing from our witnesses today on how we can do this. And I plan to work with my colleagues on both sides of the aisle to craft strong, comprehensive privacy legislation that puts consumers first.

Ms. SCHAKOWSKY. I thank the gentleman. The gentleman yields back and now the Chair recognizes Mr. Walden, ranking member of the full committee, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Well, good morning and welcome to our Members and our witnesses and congratulations to both Representative Rodgers as the new lead Republican and to Representative Jan Schakowsky as the new chair of the Consumer Protection and Commerce Subcommittee. I know we are off to a good start this morning.

We have a lot of important issues to work on in this subcommittee and I am hopeful we can continue the bipartisan achievements out of this subcommittee from Chair Schakowsky and Representative Latta's SELF DRIVE Act to legislation focused on the Internet of Things and the oversight of the FTC, CPSC, and NHTSA. I hope we can continue working together for the benefit of the American consumer.

I would also like to thank Chairs Pallone and Schakowsky for picking up on the privacy and security issues as the topic of the first hearing for this subcommittee. From the disrupter series of hearings that we held in the last Congress to the first congressional hearings with major tech companies' CEOs, this committee has been on the forefront of getting answers for our constituents.

The debate over privacy, it is not new. From the first Kodak camera to caller ID, major privacy debates ensued when new innovation was introduced. But there are new challenges when it comes to privacy, and we have heard some of that today from our Members. Privacy means different things to different people, which makes this debate even more challenging in the age of Instagram and YouTube.

I believe it is important that we work together toward a bipartisan Federal privacy bill that, one, improves transparency, accountability, and security for consumers; that, two, protects innovation and small businesses; and, three, sets one national standard. Now the first issue, as some like to frame as incredibly divisive, falls under the most basic principle underpinning our jurisdiction, and that is the term "interstate commerce."

A Federal privacy bill needs to be just that, one that sets the national standard for commercial collection use and sharing of personal data in the best interest of consumers. The Supreme Court has recently reaffirmed the principles of the commerce clause. State laws cannot discriminate against interstate commerce. They cannot impose undue burdens on interstate commerce and should take into consideration the small businesses startups and others who engage in commerce across State lines.

There are many policy areas where it makes sense for States to innovate. However, the internet does not stop at a State line and

neither should innovative privacy and security solutions. Your privacy and security should not change depending on where you live in the United States. One State should not set the standards for the rest of the country.

We can improve the security and privacy of consumers' data without adding to the confusion or harming small businesses and entrepreneurs, so Congress should thoughtfully consider what various States are proposing so we can deliver that certainty and do so with a national standard. We can learn from California and we can learn from Washington and a growing number of other States who have drafted their own legislation reinforcing why we should begin with an agreement that a Federal privacy bill sets one national standard.

Now a truly American approach to privacy and security can give consumers better control by supporting innovative solutions without massively expanding the regulatory State. We should avoid creating a system that floods people's inboxes with privacy policies that frankly they do not read, or click through notices that even make simple tasks very frustrating. We can and should, however, learn from previous efforts here at home and abroad.

So transparency and accountability are critical to move forward and measurably improve consumers' ability to choose between services they want to use. People need to receive a clearer understanding of exactly how their data are used by the digital services with whom they interact. The FTC has announced their investigation into both Equifax and Facebook. The outcome of their work will help Congress evaluate the effectiveness of laws currently on the books and the enforcement tools utilized to hold companies accountable. We can write bill after bill and the FTC can publish rule after rule, but if we do not have effective enforcement, they are just rules on paper.

So I believe we have a unique opportunity to address some of the most complex privacy and security questions of the day and I look forward to working with my colleagues across the aisle on setting a national framework and getting this debate moving forward toward a bipartisan national solution. With that, Madam Chair, I yield back.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Good morning. Welcome to our Members and witnesses.

Congratulations to both Representative Rodgers as the new lead Republican, and to Representative Schakowsky as the new chair for the Consumer Protection and Commerce Subcommittee.

We have a lot of important issues to work on in this subcommittee, and I am hopeful we can continue the bipartisan achievements out of this subcommittee. From Chair Schakowsky and Rep. Latta's SELF DRIVE Act, to legislation focused on the Internet of Things, and oversight of the FTC, C.P.S.C. and NHTSA, I hope we can continue working together for the benefit of the American consumer.

I would like to thank Chairs Pallone and Schakowsky for picking up the privacy and security issues as the topic of the first hearing for the subcommittee. From the Disrupter Series of hearings, to the first congressional hearings with major tech company CEOs, this committee has been on the forefront of getting answers for our constituents.

The debate over privacy is not new. From the first Kodak camera to caller-ID, major privacy debates ensued when they were introduced. But there are new challenges when it comes to privacy. Privacy means different things to different people,

which makes this debate even more challenging in the age of Instagram and YouTube stars comfortably sharing their most private moments in real time.

I believe it is important that we work together toward a bipartisan Federal privacy bill that: improves transparency, accountability, and security for consumers; protects innovation and small businesses; and sets one national standard.

The first issue, that some like to frame as incredibly divisive, falls under the most basic principle underpinning our jurisdiction: interstate commerce. A Federal privacy bill needs to be just that: one that sets the national standard for commercial collection, use, and sharing of personal data in the best interest of consumers.

The Supreme Court has recently reaffirmed the basic principles of the Commerce Clause: State laws cannot discriminate against interstate commerce, they cannot impose undue burdens on interstate commerce, and should take into consideration the small businesses, startups, and others who engage in commerce across State lines.

There are many policy areas where it makes sense for States to innovate; however, the internet does not stop at State lines and neither should innovative privacy and security solutions. Your privacy and security should not change depending on where you are in the United States. One State should not set the standards for the rest of the country. We can improve the security and privacy of consumers' data without adding to the confusion or harming small businesses and entrepreneurs—so Congress should thoughtfully consider what various States are proposing so we deliver that certainty with a national standard.

We can learn from California, Washington, and a growing number of other States who have drafted their own legislation—reinforcing why we should begin with an agreement that a Federal privacy bill sets one national standard.

A truly American approach to privacy and security can give consumers better control by supporting innovative solutions without massively expanding the regulatory state. We should avoid creating a system that floods people's inboxes with privacy policies they do not read or click-through notices that make even simple tasks frustrating. We can, and should, learn from previous efforts here at home and abroad.

Transparency and accountability are critical to move forward and measurably improve consumers ability to choose between services they want to use. People need to receive a clearer understanding of exactly how their data are used by the digital services with whom they interact.

The FTC has announced their investigations into both Equifax and Facebook. The outcome of their work will help Congress evaluate the effectiveness of laws currently on the books, and the enforcement tools utilized to hold companies accountable. We can write bill after bill, and the FTC could publish rule after rule, but if we do not have effective enforcement, they are just words on paper.

I believe we have a unique opportunity to address some of the most complex privacy and security questions of our day.

I look forward to working with my colleagues across the aisle on setting the framework for this debate and moving forward towards a bipartisan national solution.

Thank you and I yield back.

Ms. SCHAKOWSKY. Thank you. The gentleman yields back. And the Chair would like to remind Members that pursuant to committee rules, all Members' written opening statements shall be made part of the record.

And now I would like to introduce our witnesses for today's hearing and thank you all for coming. We have Ms. Brandi Collins-Dexter, senior campaign director, media, democracy and economic Justice, at Color of Change; Dr. Roslyn Layton, visiting scholar at the American Enterprise Institute; Ms. Denise Zheng—is that correct, “Zhong”? OK—vice president, technology and innovation, Business Roundtable; Dr. Dave Grimaldi, executive vice president for public policy, IAB; and Dr. Nuala O'Connor, president and CEO at the Center for Democracy & Technology.

And let's begin then with Ms. Collins-Dexter.

STATEMENTS OF BRANDI COLLINS-DEXTER, SENIOR CAMPAIGN DIRECTOR, COLOR OF CHANGE; ROSLYN LAYTON, PH.D., VISITING SCHOLAR, AMERICAN ENTERPRISE INSTITUTE; DENISE E. ZHENG, VICE PRESIDENT, TECHNOLOGY AND INNOVATION, BUSINESS ROUNDTABLE; DAVID F. GRIMALDI, JR., EXECUTIVE VICE PRESIDENT, PUBLIC POLICY, INTERACTIVE ADVERTISING BUREAU; AND NUALA O'CONNOR, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CENTER FOR DEMOCRACY & TECHNOLOGY

STATEMENT OF BRANDI COLLINS-DEXTER

Ms. COLLINS-DEXTER. Good morning Madam Chair, Ranking Member Rodgers, Committee Chairman Pallone, Committee Ranking Member Walden, and members of the subcommittee. My name is Brandi Collins-Dexter, and I am a senior campaign director at Color of Change, the largest online civil rights organization in the United States with more than 1.5 million members who use technology to fight for change.

In the wild, wild West of the digital economy, discriminatory marketing practices are so lucrative that entire industries have sprung up to discriminate for dollars. One company called Ethnic Technologies—subtle, I know—developed software that predicts an individual's ethnic origin based on data points easily purchased from ISPs and then sells that data, which has been turned into a predictive algorithm, to any company that wants to target groups or services to a particular ethnic group. Part of what we are seeing now is bad online behavior that circumvents civil rights laws.

Google and Facebook have both had numerous complaints filed against them for allowing discriminatory housing and employment ads. State commission reports found that voter suppression ads were specifically targeted towards black Americans on social media during the 2016 Presidential election and that social media companies made misleading or evasive claims about those efforts.

Additionally, low-income communities are targeted by predatory payday loan companies that make billions of dollars in interest and fees on the back of struggling families. We have seen online price gouging and digital redlining where corporations like Staples have used geotracking and personal data to charge customers higher prices for products based on their geography. Some data brokers even lump consumers into categories like, quote unquote, getting by, compulsive online gamblers. One company has even used a category called "Speedy Dinero," described as, quote, "Hispanic communities in need of fast cash receptive to some prime credit offers."

Last week, as was mentioned, Facebook was caught obtaining sensitive personal information submitted to entirely separate mobile apps using software that immediately shares data with social networks for ad targeting. I mean, literally, my iPad knows more about me than my husband and he is an ex-journalist who is very nosy. Even information that feels innocuous can become a proxy for a protected class. And sensitive information, right now corporations are able to easily combine information about you that they have purchased and create a profile of your vulnerabilities.

Earlier this month, Color of Change joined with advocacy groups to urge Congress to put civil and human rights at the center of the

privacy fight. Our letter states in part, “Civil rights protections have existed in brick and mortar commerce for decades. Platforms and other online services should not be permitted to use consumer data to discriminate against protected classes or deny them opportunities in commerce, housing, and employment, or full participation in our democracy.”

There are many bills out there, some we think are weak and some like language we have seen from Senator Cortez Masto, so a great deal of promise. But ultimately we would like to see bipartisan legislation written through an antidiscrimination lens that prevents manipulative or exclusionary marketing practices that exacerbate poverty. It should offer a baseline that does not preempt innovative State policy and it must contain enforcement mechanisms and not rely on self-regulation.

Some say privacy is the currency you pay to engage in our digital ecosystem. We should not have to make that choice. Our communities need to trust that when we go online we can count on our privacy and the safety of our information for ourselves and our children. This shouldn’t be a game of political football. Eighty percent of Americans support making it illegal for companies to sell or share their personal information. At least 80 percent of us believe that we should have control over how companies use our information.

Privacy is a concept in its most aspirational sense. It is not merely about the freedom and ability to close your digital curtain, so to speak. Instead, we should consider privacy and digital rights for all a necessary framework crucial for ensuring that our human, civil, and constitutional rights are not confined to our offline lives, but are also protected online where so much of our daily life occurs. I would even say that if we fail in the mission to ensure our rights online are protected, we stand to render many of our offline rights meaningless.

Thank you again for having me here today, and I look forward to your thoughts.

[The prepared statement of Ms. Collins-Dexter follows:]



**TESTIMONY OF BRANDI COLLINS-DEXTER
Senior Campaign Director, Color Of Change**

**Before the
Subcommittee on Consumer Protection and Commerce
United States House Committee on Energy and Commerce**

Hearing on "Protecting Consumer Privacy in an Era of Big Data"

February 26, 2019

Good morning Chairwoman Schakowsky, Ranking Member Rodgers, and Members of the subcommittee.

My name is Brandi Collins-Dexter, and I am a senior campaign director at Color Of Change. Color Of Change is the nation's largest online civil rights organization in the United States, with more than a 1.5 million members who use technology to fight for change.

We motivate our members – and hopefully their friends and family – to believe in a better world and join campaigns for systemic change across many key domains of Black community life in service of dignity, equity, opportunity and justice. I'm here today representing the voices of our members because the privacy fight in the internet age cuts across many, if not all, of those planks, including economic justice, media justice, criminal justice and democratic freedom. Setbacks for net neutrality, threats to privacy, and increasing surveillance continue to compromise the potential the internet has as a venue to amplify voices from traditionally marginalized communities. Whether intentional or unintentional, the tracking of users across the web and what happens to that data disproportionately impacts communities of color.

A few grounding facts- Black and Brown families use many social media platforms at higher rates, including Twitter, Instagram and WhatsApp (both owned by Facebook), and YouTube (owned by Google). Children, teens, people who are low-income, and Black and Brown people regardless of economic status rely more on their smartphones than others as their primary device to use the internet —meaning they may share detailed information about their whereabouts, their contacts, and their communications with the tech giants that provide mobile operating systems and applications. Black and Brown communities also over index on androids, unable to afford the built-in anonymized data and encryption protections offered by iPhones. This leaves Black and Brown communities grappling with how to engage with platforms not built for, operated by or meant for us.

The growth of the tech giants has led directly to a concentration of control over communications platforms that are now fundamental to participation in democracy, the



economic marketplace, and civil society. People say that in some countries, Facebook *is* the internet- but there are many communities right in here in the US where the same is true. For most people, their circle of communication can be restricted to their neighborhood, their workplace and what they experience on Facebook. It's a tension that we have to struggle against. Particularly, Facebook's model is centered around continual growth, being able to monetize data in increasingly personalized and specific ways, and being able to shape public sentiment in any number a ways- regardless of how actively one engages with the product.

But Facebook does not stand alone. Tech giants, including Google and Amazon, and Internet Service Providers like Comcast and Verizon, have grown so large, so quickly that they have completely overtaken vital institutions and industries, leaving little room for anyone to compete who is not an already-established corporate actor. These companies have gained their dominance in part through anti-competitive practices, such as acquiring emerging competitors, practicing predatory pricing, exploiting workers, and taking advantage of the power of network effects to cement their positions.

Even if we think some of the information we share may feel innocuous, our data can easily become a proxy for protected class and sensitive information. Right now corporations are able to easily combine information about you that they've purchased, and create a profile of your vulnerabilities. Algorithms, which increasingly drive consumer and employee access, work as a kind of black box that can drive exclusionary practices. Artificial Intelligence and algorithms rely on assumptions about behavior, these programs then often embed stereotypes into technology, such as facial recognition software that routinely misidentifies people of color and algorithms that racialize search results for people or businesses.

Some examples of key impacts:

- Proxies for race, including name and geo-targeted advertising, often result in discriminatory employment, advertising and marketing practices.
 - Staples, Home Depot, Discover Financial Services and Rosetta Stone, have all been found to use information on user physical locations to display different online prices to different customers. Instead of doing this to benefit those living at or below the poverty line, higher-income locations are offered better deals, while those in poorer areas are forced to pay more with fewer alternatives.
 - Credit card companies like Capital One show different offers with different credit card deals based on view locations and guesses by the company about their income.
 - Googling Black sounding names is also more likely to trigger ads for criminal databases, leading the mind to associate the name with criminality. This can lead



to loss of employment and housing opportunities, particularly for young people and teenagers newly on the job or housing market.

- Sensitive information and changes in daily habits are tracked and sold to third party data mining companies and marketers.
 - Internet Service Providers and third party analytics partners can track the times when someone goes online, the sites visited and the physical location. So when a home connection that's normally dormant during the day, suddenly becomes active and the sites visited include job search sites, the ISP can infer a subscriber has lost their job. Without regulation that information can be sold to predatory financial vendors.
 - Similar to the example above, visits to a doctor's website or to a prescription refill page could allow the ISP, platform, or a data broker partner to infer someone in the household has a specific medical condition. That information could be sold without consent to pharmaceutical and healthcare companies or even potential employers without the consent or authorization of the user.
- Advertising targeted to children circumvent established rules and guidelines enacted for the their safety.
 - A resurgence of predatory junk food marketing practices online regularly violates decades old regulations for children's television.
 - University of California-Berkeley found that thousands upon thousands of children's apps available on Google play violated The Children's Online Privacy Protection Act.
 - Tech giants have also intentionally designed products to be addictive and inescapable. This leads to a cascade of other problems, including heightened rates of depression, suicide, and sleep deprivation among young people.
- People in abusive relationships are exposed to digital methods of targeting, tracking and stalking, endangering their mental and physical health and safety.
 - More than 200 apps and services offer potential stalkers a number of capabilities, from location tracking to harvesting texts and even secretly recording video. Over two dozen services are actively promoted as surveillance tools for spying on romantic partners.
 - With the rise of the Internet of Things, the information about everyday habits that can be tracked will continue to grow and put our safety and information increasingly at risk. Traditional home appliances and parts—from thermostats to televisions to door locks—are already "smart." Cars are now commonly Internet-equipped. According to a report from the New York Times last year, these are all routinely used as a means for harassment, monitoring, revenge and control.

These are just a few examples. That's why earlier this month, Color Of Change joined with 40 advocacy groups to urge congress to put civil and human rights at the center of the privacy fight.



We offered a number of principles that I would like to share here, but are included more in depth as an addendum to my testimony.

1. Stop High-Tech Profiling and the rampant use of digital stop and frisk disproportionately targeted towards communities of color.
2. Ensure Fairness in Automated Decisions. Look at the impact of computerized decision making in the areas of employment, health, education and lending.
3. Preserve Constitutional Principles. Digital tools, platforms and tracking should not be used to circumvent due process, warrants, or other independent oversight of law enforcement. Government databases must not be allowed to undermine privacy and freedom of association.
4. Enhance Individual Control of Personal Information. Individuals should have meaningful, flexible control over how a corporation gathers data from them, and how it uses and shares that data. Non- public information should not be disclosed to the government without judicial process.
5. Protect People from Inaccurate Data. Government and corporate databases must allow everyone the ability to ensure the accuracy of personal information that is used to make important decisions about them. This requires disclosure of the underlying data, and the right to correct it when inaccurate.

Ultimately, privacy as a concept in its most aspirational sense is not merely about the freedom and ability to close your "digital curtains" so no one can peek in. Instead, I would respectfully challenge all of us to consider privacy and digital rights for all as a necessary framework crucial to ensuring that our human, civil and constitutional rights are not confined to our offline lives but are also protected online where so much of our daily life occurs. I would even say that if we fail in the mission to ensure our rights online are protected, we stand to render many of our offline rights meaningless.

Strong privacy rules are crucial to ensuring economic growth and opportunity, informed consumer choices and data protection. It has become increasingly clear by the day that decision makers have to do better. Strong privacy rules passed by the Federal Communications Commission were obliterated in 2017, leaving a wide open lane for an explosion of unchecked predatory practices. The Federal Trade Commission currently has no power to enact privacy rules since they have no jurisdiction over Internet Service Providers; their privacy framework is a non-binding set of recommendations that require industry self-regulation; and they have shown an unwillingness to forcefully exert what power they do have. What we need is clear, federal baseline legislation that does not preempt innovative state policy laws but ensures basic rights for everyone in the United States. A basic framework should do the following:

- o Establish limits on the collection, use and disclosure of sensitive personal data;
- o Establish enhanced limits on the collection, use and disclosure of data of children and teens;



- Regulate consumer scoring and other business practices that diminish people's physical health, education, financial and work prospects;
- Prohibit or prevent manipulative marketing practices; and
- Establish a data protection agency that is empowered to ensure that privacy rights are protected through enforcement mechanisms.

More about a proposed framework developed in partnership with several privacy groups is also included in the addendum to this testimony.

Finally, I'd like to mention one more document included for your reference, the Our Data Bodies project. The Our Data Bodies Project focused on three cities and interviewed people on the ground about their feelings and concerns about how data intersects with our daily lives: in Charlotte they focused on the relationship between data, re-entry and processes like applying for a job; in Los Angeles, interviewees came from communities like Skid Row and face housing insecurity and issues with public benefits; while in Detroit, themes emerged around data, foreclosures, evictions and utility shut-downs. It's an unfiltered, at times rough, but candid look at the impact of data collection and data-driven systems on the ability of marginalized peoples to meet their human needs. The frustrations are clear and as you read through it, it serves as a reminder of the ways beyond pieces of our whole selves are collected, stored in databases, the cloud, and other spaces of digitally networked flows, and used to make decisions or determinations about us.

I have heard it said that privacy is the currency you pay to engage in our digital ecosystem. We should not have to make that choice. Our communities need to trust that when we go online, we can count on our privacy and the safety of our information for ourselves and for our children. This shouldn't be a game of political football- 80% of Americans support making it illegal for companies to sell or share their personal information. At least 80% of us believe that we should have control over how these companies use our personal information.

Ultimately, I do not envy the work ahead of you all. The reality is that no one intervention will magically wipe away inequities, if such a magic concoction existed, I would like to think we would have all taken it by now. But I and others have done our best to offer a set of principles and an aspirational framework as your north star. My hope is that you will be guided by an unwavering desire to ensure that hard fought, bipartisan, civil rights wins of the past are not undermined, models of discrimination are not replicated online and that we all have ability to take advantage of all the opportunities a safe and secure internet can offer.

Thank you for your time, I look forward to your thoughts.

[Ms. Collins-Dexter's entire statement, including supplemental material that does not appear in the printed edition, has been retained in committee files and also is available at <https://docs.house.gov/meetings/IF/IF17/20190226/108942/HHRG-116-IF17-Wstate-Collins-DexterB-20190226.pdf>.]

Ms. SCHAKOWSKY. Thank you. I meant to mention that each of you has 5 minutes, and I appreciate you, Ms. Collins-Dexter, for sticking to that. The lights that will go on initially will be green, and then the light will turn yellow when you have 1 minute remaining, and then red means you need to stop.

And so, Dr. Layton, you are recognized for 5 minutes.

STATEMENT OF ROSLYN LAYTON

Dr. LAYTON. Good morning. Thank you, Chair Schakowsky, Ms. McMorris Rodgers, and members of the committee. It is an honor to be here, and I am heartened by your bipartisanship.

Today I represent only myself and my research. I have lived in the European Union for the last decade, and I work at a European university where I make international internet policy comparisons. As the mother of three Danish-American children, I am legitimately interested in policy that makes Europe a better place.

The academic literature shows that online trust is a function of institutions, business practices, technologies, and users' knowledge. But unfortunately the EU rejected this formula for its data protection policy. My hope is that Congress will avoid the mistakes of the GDPR and ultimately leapfrog Europe with a better framework based upon privacy-enhancing technologies, a strong Federal standard, and consumer education.

To analyze a policy like the GDPR we must evaluate its real-world effects. Since its implementation, Google, Facebook, and Amazon have increased their market share in the EU. This is a perverse outcome for a policy promised to level the playing field. Today, only 20 percent of EU companies are online. There is little to no data that shows that small and medium-sized enterprises are gaining as a result of the GDPR.

The data shows a consistent lag in the small to medium-sized business segment particularly for them to modernize their websites and market outside their own EU country. Now this outcome isn't necessarily surprising. As a Nobel Prize economist, George Stigler, observed 40 years ago, regulation is acquired by industry and operated for its benefit. A number of large companies have come out in support of the GDPR. It doesn't surprise me either, that is because it cements their market position. They don't need permissionless innovation anymore, but they don't have a problem depriving startups of the same freedom.

Now to comply with the GDPR today, an average firm of 500 employees will spend about \$3 million. And thousands of U.S. firms have decided that this is not worthwhile, including the Chicago Tribune, which is no longer visible in the European Union. There are over 1,000 American news media that no longer reach Europeans. This is also concerning because the EU is the destination of two-thirds of America's digital goods and services.

Now the GDPR might be justified if it created greater trust in the digital ecosystem, but there is no such evidence. After a decade of these kinds of data protection regulations in the EU, in which users endure intrusive pop-ups and disclosures in every digital site they visit, Europeans report no greater sense of trust online. More than half of the survey respondents in the UK alone say that they

feel no better since the GDPR took effect and it has not helped them to understand how their data is used.

I am skeptical of both the GDPR and the CCPA in California with their laundry list of requirements, 45 in Europe and 77 in California. These are not scientifically tested and there is no rational policy process to vet their efficacy. Now I imagine if we held—now what would happen if we would hold government to the same standards? Australia tried a “when in doubt, opt out” policy and half a million people left the national healthcare record program. It crashed their system for healthcare.

We have another reason to be skeptical of the claims of the EU being morally superior with their GDPR. Their networks are not secure because they are built with equipment by dubious Chinese equipment makers. Your data protection standard means little if the Chinese Government can hack your data through back doors.

In any event, Europe’s attempt to create a common market for data is something that was actually part of our founding and of our country with our national standard in interstate commerce, which has been discussed, and I support such a national standard for sensitive data consistently applied across enterprises. To leap the Europeans on data protection we need to review the empirical research that the Europeans ignored, namely how privacy-enhancing technologies and user knowledge will promote online trust.

The answer is not to copy the EU, but to build world-class, scientifically superior, privacy-enhancing technologies here in the United States. Congress should incentivize the development of such technologies through grants and competitions and provide safe harbors for their research, development, and practice. There is no consumer protection without consumer education and we should support people to acquire their digital competence so they make informed decisions about the products they use.

In closing, please do not fall prey to the European regulatory fallacy which substitutes the bureaucratization of data instead of a natural right of privacy. Increasing the number of agencies and bureaucrats who govern our data does not increase our privacy. It reduces our freedom, makes enterprise more expensive, and deters innovation. Thank you for your leadership. I welcome your questions.

[The prepared statement of Dr. Layton follows:]



Statement before the House Committee on Energy and Commerce
Subcommittee on Consumer Protection and Commerce
On Protecting Consumer Privacy in the Era of Big Data

How the US Can Leapfrog the EU

The Role of Technology and Education in Online Privacy

Roslyn Layton
Visiting Scholar

February 26, 2019

The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the author.

Chair Schakowsky, Ranking Member McMorris Rodgers, and Members of the Committee, thank you for the opportunity to discuss protecting consumer privacy in the era of Big Data. It is an honor. I am heartened by your bipartisanship on this important issue.

My testimony is informed by working in this field for more than a decade, including at a European university. My academic research explores online privacy as a comprehensive framework incorporating institutions, business practices, the type of technologies, and, most important, the level of the user's knowledge.¹ As a mother of three Danish-American children, I also have a personal interest in whether the European rules work.

My goal is for Congress to learn about the results of the General Data Protection Regulation (GDPR), avoid its mistakes, and ultimately leapfrog Europe with a better framework. In this testimony, I will discuss privacy-enhancing technology and competition, data security, the importance of a strong federal standard, and the role of consumer education.

How Privacy-Enhancing Technologies Can Promote Competition

Many Americans are persuaded by lofty descriptions of the GDPR—contrasting the legislation with what they see as a morally inferior *laissez faire* approach at home—both because they confuse data privacy and protection and because they are not familiar with America's own substantive protections. Journalists and commentators glibly refer to the US as the “Wild West,” as if there are no laws or regulation on data privacy and protection.² In fact, there are literally hundreds of laws relating to privacy and data protection in the US—including common law torts, criminal laws, evidentiary privileges, federal statutes, and state laws.³ The EU's laws are relatively new, officially dating from this century, and they still lack the runway of judicial scrutiny and case law that characterizes US law.

A popular misconception about the GDPR is that it protects privacy; it does not. In fact, the word “privacy” does not even appear in the final text of the GDPR, except in a footnote.⁴ Rather, the GDPR is about data protection or, more correctly, data governance.⁵ Data privacy is about the use of data by people who are allowed to have it. Data protection, on the other hand, refers to technical systems that keep data out of the hands of people who should not have it. By its very name, the GDPR regulates the processing of personal data, not privacy.

The American notion of privacy is predicated largely on freedom from government intrusion and as a counterweight to the growth of the administrative state.⁶ The Bill of Rights' Third, Fourth, and Fifth Amendments responded to the egregious British abuses of personal privacy, including the quartering of soldiers in private homes, the search and seizure of colonists' property, and forcing colonists to divulge information. Some of the first laws in the new republic were enacted

to protect privacy in mail. These were followed by laws constraining the government's use of the census⁷ and its ability to compel information in court.⁸ The 1966 Freedom of Information Act ensured that people could access records held by the government. Given this history of pushing back against government intrusion, it is reasonable to be skeptical that increasing government power is now the key to privacy in the US.

To analyze a policy like the GDPR, we must set aside the political pronouncements and evaluate its real-world effects. Since the implementation of the GDPR, Google, Facebook, and Amazon have increased their market share in the EU.⁹ In spite of some years of notice about the GDPR's coming implementation, only 20 percent of EU companies, primarily the large firms, are digitized.¹⁰ There is little to no data that shows that small to medium sized companies are growing in the EU as a result of the regulation.¹¹ The European Commission's Digital Scoreboard reports shows a consistent lag in the SME segment, particularly to modernize their websites and market outside their own EU countries.¹² One study suggests that small- and medium-sized ad tech competitors have lost up to one-third of their market position since the GDPR took effect.¹³ The GDPR does not bode well for cutting-edge firms, as scientists describe it as fundamentally incompatible with artificial intelligence and big data.¹⁴ This is indeed a perverse outcome for a regulation that promised to level the playing field.

But for those who study the empirical outcomes of regulation, it is not a surprise. As Nobel Prize Economist George Stigler observed more than 40 years ago, "Regulation is acquired by industry and operated for its benefit."¹⁵ The GDPR is a barrier to market entry that punishes small firms, rewards large ones, and creates a cozy relationship between regulators and the firms they regulate.

To do business in the EU today, the average firm of 500 employees must spend about \$3 million to comply with the GDPR.¹⁶ Thousands of US firms have decided it is not worthwhile and have exited.¹⁷ No longer visible in the EU are the *Chicago Tribune* and the hundreds of outlets from Tribune Publishing.¹⁸ This is concerning because the EU is the destination of about two-thirds of America's exports of digital media, goods, and services.¹⁹ Indeed, the GDPR can be examined as a trade barrier to keep small American firms out so that small European firms can get a foothold.²⁰

Of course, \$3 million, or even \$300 million, is nothing for Google, Facebook, and Amazon (The Fortune 500 firms have reportedly earmarked \$8 billion for GDPR upgrades.²¹), but it would bankrupt many online enterprises in the US. Indeed, less than half of eligible firms are fully compliant with the GDPR; one-fifth say that full compliance is impossible.²² The direct welfare loss is estimated be about €260 per European citizen.²³ If a similar regulation were enacted in

the US, total GDPR compliance costs for US firms alone could reach \$150 billion, twice what the US spends on broadband network investment²⁴ and one-third of annual e-commerce revenue in the US.²⁵

The GDPR has affected not just American media outlets, but also their advertisers. Given the scope of Google's advertising platform and its affiliates on syndicated networks, its compliance with the GDPR has caused ripple effects in ancillary markets. Independent ad exchanges noted prices plummeting 20 to 40 percent.²⁶ Some advertisers report being shut out from exchanges.²⁷ The GDPR's complex and arcane designations for "controllers" and "processors" can ensnare third-party chipmakers, component suppliers, and software vendors that have never interfaced with end users, as European courts have ruled that any part of the internet ecosystem can be liable for data breaches.²⁸

Many American retailers, game companies, and service providers no longer operate in the EU. The Williams-Sonoma and Pottery Barn websites are dark.²⁹ The San Francisco-based Klout, an innovative online service that used social media analytics to rate its users according to online social influence, closed down completely.³⁰ Drawbridge, an identity-management company from San Mateo, California, exited the EU and sold off its ad-tracking business because of the GDPR.³¹ Verve, a leading mobile marketing platform with offices in six US cities, closed its European operation in advance of the GDPR, affecting 15 EU employees.³²

Valve, an award-winning video game company in Bellevue, Washington, shut down an entire game community rather than invest in GDPR compliance.³³ Uber Entertainment, also based in Washington, similarly shut down one of its most popular games entirely after a six-year run because upgrading the platform to GDPR compliance was too expensive.³⁴ California-based Gravity Interactive no longer offers games in the EU and refunded its European customers.³⁵

The Las Vegas-based Brent Ozar Unlimited, which offers a range of information technology and software support services, stopped serving the EU.³⁶ San Francisco's Payver, the dashboard camera app that pays drivers to collect road information on potholes, fallen road signs, and other inputs to build maps to improve the safety of self-driving cars, no longer supports the EU.³⁷ Legal news website Above the Law describes the EU closures of Ragnarok Online, Unroll.me, SMNC, Tunngle, and Steel Root, noting that the GDPR is splintering the internet and that GDPR policymakers refused to listen to concerns from startups before the launch and now refuse to fix its problems.³⁸ Even the Association of National Advertisers website is not available in the EU.³⁹

The regulation has hurt European venture capital. An important study published by the National Bureau of Economic Research and coauthored by the Federal Trade Commission's (FTC) former chief economist notes a \$3.38 million decrease in total dollars raised per country per week from

July 2017 to September 2018, a 17.6 percent reduction in weekly venture deals, and a 39.6 percent decrease in the amount raised per deal. The numbers are associated with between 3,000 and 30,000 job losses.⁴⁰

The GDPR might be justified if it created greater trust in the digital ecosystem, but there is no such evidence. After a decade of GDPR-type regulations—in which users endure intrusive pop-ups and disclosures on every digital property they visit⁴¹—Europeans report no greater sense of trust online.⁴² More than half of survey respondents in the United Kingdom say that they feel no better off since the GDPR took effect and that it as not helped them understand how their data is used.⁴³ As of 2017, only 30 percent of Europeans shop outside their own country (a paltry increase of 10 percent in a decade), demonstrating that the European Commission’s Digital Single Market goals are still elusive.⁴⁴

The other misconception of the GDPR is that its grab bag of 45 enterprise regulations magically delivers consumer protection, but these have not been tested scientifically. Regulation ensures compliance to an explicit mandated standard, not consumer protection, something that by definition varies from person to person. As such, I am similarly skeptical of the California Consumer Privacy Act (CCPA), which has even more enterprise requirements—77.

Indeed, if EU and California provisions were so laudable, why are we not demanding that American government institutions also uphold these standards? Such rules would likely cripple, both logistically and financially, the hundreds of personal data-collection agencies of the federal government and thousands in state and local government. With the mantra of “if in doubt, opt out,” about half a million Australians rejected that country’s national electronic health record, causing the federal computer system to crash in July 2018 and casting doubt on the underlying economics of the model.⁴⁵

What then can policymakers do to ensure that policies promote competition? For one, they can ensure that the privacy framework does not unduly burden small and medium sized firms. Policies should focus on proven, legitimate practices that can prevent harm, not require compliance for a laundry list of “designer” provisions.

If anything, the policy should promote firms to use data. Indeed, the trouble with today’s economy is not that there is too much use of data, but too little. A lack of “information intensity” is holding back the so-called other 70 percent of American economy, sectors such as transportation and health care, the latter of which consumes almost one-fifth of gross domestic product.⁴⁶ Outside of certain applications, the traditional healthcare industry is woefully inefficient; digital industries are 8 times more productive and innovative. If the US does not innovate these other sectors, other nations will beat us to it. China is already on track with an “Internet Plus” policy

which supports the digitization of industries, including healthcare and government.⁴⁷

Ideally we need a technologically neutral national framework with a consistent application across enterprises. It should support consumers' expectations to have same protections on all online entities.⁴⁸ The law should make distinctions between personally identifiable information which deserves protection, but not require same high standard for public data, de-identified, and anonymized data which do not carry the same risks. Unlike the GDPR, the US policy should not make it more expensive to do business, reduce consumer freedom, or inhibit innovation.

Some of America's greatest resources are intellectual capital and creative ingenuity. We should build on our technology prowess to create world-class, scientifically superior privacy design. There are hundreds of privacy-enhancing technologies.⁴⁹ No one technology is best for all companies, and in practice, companies use a mix of technologies. Congress should incentivize the development of such technologies through grants and competitions and provide safe harbors for their research, development, and practice.

Congress should also be wary of mandates that all companies use the same technology, it removes the means for companies to compete and their incentive to innovate a better technology. Moreover, a monoculture of mandated technology is an attack surface for cyber criminals.

I commend the work by the National Institute of Standards and Technology to inform this effort.⁵⁰ Moreover, the FTC's budget and authority should be expanded to accommodate the needed economists, technologists, and other professionals to enforce privacy protections. Presently, the FTC has a mere 80 economists and 800 attorneys. The consumer-protection function of the FTC should be strengthened by aggregating the consumer protection resources now frittered across a series of federal agencies and consolidating them under one roof at the FTC.⁵¹

The Role of Data Security

I have noted the security fallout from the GDPR,⁵² but there are even more fundamental security problems. In their rush to declare moral superiority over the US, European policymakers disregarded the existential threats to privacy by network hardware manufacturers Huawei, ZTE, and Lenovo.⁵³ European authorities, wanting to get networks cheaply, blessed the construction of communications networks with equipment from dubious Chinese vendors. Data-protection standards mean little if affiliates of the Chinese government and military can access our data in the cloud, through backdoors, by hacking, or through other illicit means.

Fortunately, the US does not have this problem to the same extent. The US recognized the risk at the outset, understood that security is worth paying for, and limited its exposure to these firms. I applaud Congress for its leadership with H.R. 4747,⁵⁴ and I hope it stays the course. I

also support the role of cyber insurance to help firms assess and address security risks.⁵⁵

How Common Standards Ensure Equal Privacy Protections for All Americans

The GDPR was created to bring a single standard of data protection to the EU. If each US state makes its own rules, we will become the Balkanized Europe, which the GDPR sought to remedy. The idea of a single national market is central to America's founding and was espoused by James Madison and Alexander Hamilton.⁵⁶ This framework was essential for our country to launch and commercialize the internet economy, and today the US accounts for one-third of the world's internet economy.⁵⁷ In the process of adjudication of privacy violations, it is not fair that residents of some states get payouts while others do not. America's internet companies are national, if not global, so enforcement must proceed federally from the FTC to ensure fairness. Importantly, Congress should adopt safeguards against rent-seeking by self-interested actors to abuse consumer protection laws to enrich themselves through litigation.

The Role of Consumer Education and Meaningful Transparency

My final point is the most important: There is no consumer protection without consumer education. After a decade of increasing data-protection regulation in the EU, Europeans do not report greater trust online. This is because the EU substitutes the *bureaucratization of data protection* for the *natural right of privacy*. Increasing the number of agencies and bureaucrats who govern our data does not increase our privacy.

Moreover, making a disclosure more explicit does not give us more privacy. Our policy should support the ability for people to acquire digital competence so that they can make informed decisions about the online products and services they use. People are empowered through education, not bureaucratization.⁵⁸

While we may experience a general creepiness about growing technology, it is not inherently harmful to collect and process data from individuals and give them incentives to share. Indeed, it does not appear that policymakers have identified, let alone quantified, the harm that proposed legislation would mitigate. Moreover, there are significant costs associated with regulation, and benefits do not flow equally to consumers. While some may appreciate the regulator's heavy hand, many will find it intrusive.⁵⁹ The FTC's unfairness test with its precepts of informational injury as it applies to deception (which subverts consumer choice), financial, health/safety, unwarranted intrusion, and reputation could be a helpful tool in this regard.

Upon introduction, new technologies such as the camera, transistors, and RFID chips crept

people out, but these technologies have tremendously benefited our society. This privacy panic cycle of trust, panic, deflation, and acceptance is well-documented for more than a century.⁶⁰ When asked which has most improved life in the past 50 years, Americans note technology more than four times as often as medicine, civil rights, or the economy.⁶¹

Regulatory advocates may be noble and well-intentioned in their desire to protect consumers, but regulation is never neutral. It is subject to biased human decision-making and interpretation. Nor is regulation necessarily quick or effective. GDPR policymakers claim that it will be at least two years to conclude a major enforcement.⁶² Moreover, California, which before its CCPA already had more privacy laws than any state, does not report that its residents felt more safe, private, or secure.

I applaud President Barack Obama's leadership on his 2012 Online Bill of Rights for Consumers (and, indeed, the provisions are not controversial today).⁶³ Hundreds of privacy enforcements have been made over the years, however, it appears that certain consent decrees against major Silicon Valley companies were not enforced during his administration. Americans should not have to rely on the whims of political administrations to protect themselves. Americans should be able to choose increasingly better privacy-enhancing technologies that are divorced from politics. Moreover, the more educated people are about the technologies they use, the less they need regulators to choose for them.

I humbly submit that Congress review the empirical research on privacy and data protection that the Europeans ignored, notably the process for innovation in privacy-enhancing technologies and the primacy of user knowledge as a component of online trust.⁶⁴ The US does not need to copy the European Union on data protection. It can fundamentally improve on the GDPR by making a policy that actually works—promoting privacy without destroying prosperity, empowering people to make informed decisions, and ensuring innovators the freedom to invent and improve privacy-enhancing technology.

¹ Roslyn Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability and Trust," March 31, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944358.

² See, for example, Joe Nocera, "The Wild West of Privacy," *New York Times*, February 24, 2014, <https://www.nytimes.com/2014/02/25/opinion/nocera-the-wild-west-of-privacy.html>.

³ See Daniel J. Solove, "A Brief History of Information Privacy Law," in *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, ed. Kristen J. Mathews (New York, Practising Law Institute, 2006).

⁴ European Union, General Data Protection Regulation, note 18, <https://gdpr-info.eu/>.

⁵ Evidon, "What Is the GDPR?," <https://www.evidon.com/education-portal/videos/what-is-the-gdpr/>.

⁶ See Solove, "A Brief History of Information Privacy Law," 1-5, 1-6.

⁷ See Solove, "A Brief History of Information Privacy Law," 7.

⁸ See, for example, *Boyd v. United States*, 116 US 616 (1886).

⁹ Mark Scott, Laurens Cerulus, and Laura Kayali, "Six Months in, Europe's Privacy Revolution Favors Google, Facebook," *Politico*, November 27, 2018, <https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/>.

¹⁰ European Commission, "Integration of Digital Technology," 2018, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/4_desi_report_integration_of_digital_technology_B618EB6B-F21D-9DD7-72F1FAA836E36515_52243.pdf.

¹¹ <https://ec.europa.eu/digital-single-market/en/digital-scoreboard>

¹² European Commission, "Better Access for Consumers and Business to Online Goods," 2015, <https://ec.europa.eu/digital-single-market/en/better-access-consumers-and-business-online-goods>.

¹³ Björn Grelf, "Study: Google Is the Biggest Beneficiary of the GDPR," *Cliqz*, October 10, 2018, <https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr>.

¹⁴ For further discussion on how GDPR blocks innovation, see Roslyn Layton and Julian Mclendon, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," *Federalist Society Review* 19 (October 29, 2018): 245, <https://fedsoc-cms-public.s3.amazonaws.com/update/pdf/nv29MXrvrqabIN7n8h6WzAJ9yhbZBKITKOM-wMzVe.pdf>.

¹⁵ George Stigler, "The Theory of Economic Regulation," *Bell Journal of Economics* 2, no. 1 (1971): 3–21.

¹⁶ International Association of Privacy Professionals, "IAPP-EY Annual Governance Report 2018," 2019, <https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/>.

¹⁷ Jeff South, "More Than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect," *Nieman Lab*, August 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/>.

¹⁸ Barbara Kollmeyer, "Chicago Tribune, Los Angeles Times Go Dark in Europe After GDPR Fail," *MarketWatch*, May 25, 2018, <https://www.marketwatch.com/story/chicago-tribune-la-times-go-dark-in-europe-after-gdpr-fail-2018-05-25>.

¹⁹ US International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, August 2017, https://www.usitc.gov/publications/332/pub4716_0.pdf.

²⁰ Daniel Lyons, "GDPR: Privacy as Europe's Tariff by Other Means?," *AEIdeas*, July 3, 2018, <http://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/>.

²¹ <https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/>

²² International Association of Privacy Professionals, "IAPP-EY Annual Governance Report 2018."

²³ Hosuk Lee-Makiyama, "The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs," in *Protection of Information and the Right to Privacy—A New Equilibrium?*, ed. Luciano Floridi (Springer, 2014), 85–94. This methodology is expanded in Erik Van der Marel et al., "A Methodology to Estimate the Costs of Data Regulations," *International Economics* 146 (2016): 12–39.

²⁴ Jonathan Spalter, "Broadband CapEx Investment Looking Up in 2017," *USTelecom*, July 25, 2018, <https://www.ustelecom.org/blog/broadband-capex-investment-looking-2017>.

²⁵ US Census Bureau, "Quarterly Retail E-Commerce Sales 1st Quarter 2018," May 17, 2018, <https://www2.census.gov/retail/releases/historical/ecommm/18q1.pdf>.

²⁶ Jessica Davies, "The Google Data Protection Regulation: GDPR is Strafing Ad Sellers, *Digiday* (June 4, 2018), <https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/>.

²⁷ Catherine Armitage, "Life After GDPR: What Next for the Advertising Industry?," *World Federation of Advertisers*, July 10, 2018, <https://www.wfanet.org/news-centre/life-after-gdpr-what-next-for-the-advertising-industry/>.

²⁸ European Union, Judgment of the Court (Grand Chamber), June 5, 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0210&qid=1531145885864&from=EN>.

²⁹ Associated Press, "Amid Confusion, EU Data Privacy Law Goes into Effect," *WTOP*, May 25, 2018, <https://wtop.com/news/2018/05/amid-confusion-eu-data-privacy-law-goes-into-effect/>.

³⁰ Jon Russel, "RIP Klout," *TechCrunch*, May 2018, <https://techcrunch.com/2018/05/10/rip-klout/>.

³¹ Allison Schiff, "Drawbridge Sells Its Media Arm and Exits Ad Tech," *AdExchanger*, May 8, 2018, <https://adexchanger.com/data-exchanges/drawbridge-sells-its-media-arm-and-exits-ad-tech/>.

³² Ronan Shields, "Verve to Focus on US Growth as It Plans Closure of European Offices Ahead of GDPR," *Drum*, April 18, 2018, <https://www.thedrum.com/news/2018/04/18/verve-focus-us-growth-it-plans-closure-european-offices-ahead-gdpr>.

³³ Steam, "Super Monday Night Combat," <https://steamcommunity.com/app/104700/allnews/>.

- ³⁴ Owen Good, "Super Monday Night Combat Will Close Down, Citing EU's New Digital Privacy Law," Polygon, April 28, 2018, <https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr>.
- ³⁵ Warportal, "Important Notice Regarding European Region Access," <http://blog.warportal.com/?p=10892>.
- ³⁶ Brent Ozar, "GDPR: Why We Stopped Selling Stuff to Europe," December 18, 2017, <https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/>.
- ³⁷ Payver (@getpayver), "Sorry European Payver users! Come May 24th we're discontinuing Payver support in Europe due to #GDPR. Talk to your lawmakers....," Twitter, April 5, 2018, 5:30 p.m., <https://twitter.com/getpayver/status/981992477392437249>.
- ³⁸ Techdirt, "Companies Respond to the GDPR by Blocking All EU Users," Above the Law, May 11, 2018, <https://abovethelaw.com/legal-innovation-center/2018/05/11/companies-respond-to-the-gdpr-by-blocking-all-eu-users/>.
- ³⁹ George P. Sleo, "ANA Doesn't Have GDPR-Compliant Website; Says It Will Be up in 'Two Weeks,'" AdAge, June 7, 2018, <https://adage.com/article/digital/ana-misses-deadline-create-gdpr-compliant-website/313775/>.
- ⁴⁰ Jian Jia, Ginger Zhe Jin, Liad Wagman, "The Short-Run Effects of GDPR on Technology Venture Investment" (working paper, National Bureau of Economic Research, November 2018), <https://www.nber.org/papers/w25248>.
- ⁴¹ GDPR pop-up disclosures have become so intrusive that Europeans download pop-up blockers on their phones.
- ⁴² Daniel Castro and Alan McQuinn, "The Economic Cost of the European Union's Cookie Notification Policy," Information Technology & Innovation Foundation, November 6, 2014, <https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy>.
- ⁴³ GDPR three months on: Most consumers feel no better off. Marketing Week. Lucy Tesseris 24 August 2018. https://www.marketingweek.com/2018/08/24/gdpr-three-months-on/?ct_5bf3f166954e0=5bf3f16695585
- ⁴⁴ European Commission, "Use of Internet Services," 2018, 4, http://ec.europa.eu/information_society/news-room/image/document/2018-20/3_desi_report_use_of_internet_services_18E82700-A071-AF2B-16420BCE813AF9F0_52241.pdf.
- ⁴⁵ Layton and McLendon, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course."
- ⁴⁶ Bret Swanson. "Securing the Digital Frontier: Policies to Encourage Digital Privacy, Data Security, and Open-Ended Innovation." Summary of Forthcoming Report. AEI. February 2019.
- ⁴⁷ http://english.gov.cn/premier/news/2015/03/13/content_281475070887811.htm
- ⁴⁸ <http://www.aei.org/publication/fcc-privacy-regulation-will-limit-competition-market-really-needs-online-advertising/>
- ⁴⁹ For a discussion of privacy enhancing technologies, see Roslyn Layton, "Statement Before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, Market Solutions of Online Privacy," August 20, 2018, 8, https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf
- ⁵⁰ See US Department of Commerce, National Institute of Standards and Technology, "Cybersecurity Framework," <https://www.nist.gov/cyberframework>; and US Department of Commerce, National Institute of Standards and Technology, "Privacy Framework," <https://www.nist.gov/privacy-framework>.
- ⁵¹ See Layton, "Statement Before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings," 7.
- ⁵² See Layton and McLendon Supra 41, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," 246. The GDPR has created an existential security threat for the WHOIS database, a key internet function. "In addition, misapplication of the GDPR is hindering commerce and consumer protection because domain name providers are using it as an excuse to restrict access to WHOIS data, not just in the EU but also in the US and elsewhere. WHOIS data has been publicly available since the dawn of the commercial internet. It provides basic contact information for holders of domain names and is critical for online trust and accountability. Consumers and businesses use WHOIS data to confirm who is on the other side of web sites they engage with. Law enforcement agencies and other groups use WHOIS data to combat identity theft, theft of intellectual property, cyberattacks, illicit sale of opioids, sex trafficking, and other clearly illegal conduct online. ICANN's Government Advisory Committee and law enforcement agencies across the globe are already warning that consumer protection and criminal investigations are being stymied. Congress should consider requiring domain name providers to make the same WHOIS data available that they have been providing for more than 20 years."

-
- ⁵³ Roslyn Layton, "Trump Should Ignore Chinese Manufacturers' Phony Promises," *Forbes*, February 20, 2019, <https://www.forbes.com/sites/roslynlayton/2019/02/20/trump-should-ignore-chinese-manufacturers-phony-promises/#257b924d50ec>.
- ⁵⁴ Defending U.S. Government Communications Act, H.R. 4747, 115th Cong., <https://www.congress.gov/bill/115th-congress/house-bill/4747>.
- ⁵⁵ Hurwitz, Justin (Gus), *Cyberensuring Security* (September 1, 2017). Connecticut Law Review, Vol. 49, No. 5, 2017. Available at SSRN: <https://ssrn.com/abstract=3314400>.
- ⁵⁶ Roslyn Layton, "California's Privacy Proposal Failed, but It Probably Violated the Constitution Anyway," AEIdeas, September 18, 2017, <http://www.aei.org/publication/californias-privacy-proposal-failed-but-it-probably-violated-the-constitution-anyway/>. For an abbreviated version, see Roslyn Layton, "Internet Privacy Legislation," American Enterprise Institute, <http://www.aei.org/multimedia/internet-privacy-legislation-in-60-seconds/>.
- ⁵⁷ CompTIA, "IT Industry Outlook 2018," January 2018, <https://www.comptia.org/resources/it-industry-outlook-2018>.
- ⁵⁸ For a discussion of online privacy education, see Layton, "Statement Before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings," 12.
- ⁵⁹ A forthcoming event will describe the costs and benefits of digital rights, data protection, and data privacy. Society for Benefit-Cost Analysis, 2019 Annual Conference, March 13–15, 2019, <https://benefitcostanalysis.org/2019-annual-conference>.
- ⁶⁰ Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," Information Technology & Innovation Foundation, September 2015, <http://www2.itif.org/2015-privacy-panic.pdf>.
- ⁶¹ Mark Strauss, "Four-in-Ten Americans Credit Technology with Improving Life Most in the Past 50 Years," Pew Research Center, October 12, 2017, <http://www.pewresearch.org/fact-tank/2017/10/12/four-in-ten-americans-credit-technology-with-improving-life-most-in-the-past-50-years/>.
- ⁶² Jan Philipp Albrecht, "Press Conference by Jan Philipp Albrecht (Greens/EFA, DE), Rapporteur, on General Data Protection Regulation," European Parliament, June 15, 2018, <https://multimedia.europarl.europa.eu/en/albrecht-general-data-protection-regulation-1155149-A-ra>.
- ⁶³ Roslyn Layton, "A Look at the Growing Consensus on Online Privacy Legislation: What's Missing?," AEIdeas, October 29, 2018, <http://www.aei.org/publication/a-look-at-the-growing-consensus-on-online-privacy-legislation-whats-missing/>.
- ⁶⁴ European Union Agency for Network and Information Security, *Privacy and Data Protection by Design—From Policy to Engineering*, December 2014, <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

Ms. SCHAKOWSKY. Thank you.

Ms. Zheng, you are recognized for 5 minutes.

STATEMENT OF DENISE E. ZHENG

Ms. ZHENG. Thank you, Chairwoman Schakowsky, Ranking Member McMorris Rodgers, members of the subcommittee, thank you for the opportunity to testify on behalf of the Business Roundtable.

Business Roundtable represents more than 200 CEOs of the largest American companies that operate in nearly every corner of the economy including technology, telecommunications, retail, banking, health, manufacturing, automotive, and many other industries. Our companies touch virtually every American consumer. They process 16 trillion in global consumer payments each year and service roughly 40 million utilities customers across the country.

They fly more than 250 million passengers to their destinations each year and provide wireless communications and internet services to more than 160 million consumers. They sponsor nearly 70 million medical insurance memberships and deliver more than 42 million packages every single day. Data privacy is a major priority for the Business Roundtable especially as companies that rely on data and digital platforms to deliver products and services to consumers and to conduct day-to-day business operations.

That is why CEOs from across industry sectors have come together to call for a Federal privacy law that provides consistent consumer privacy protections, promotes accountability, and fosters innovation and competitiveness. We strongly support giving consumers control over how their personally identifiable information is collected, used, and shared.

At the same time, it is important to remember the value of data in our economy as well as the enormous benefits that data-driven services provide to our consumers. Data enables companies to deliver more relevant and valuable user experience to consumers. It allows companies to detect and prevent fraud on user accounts and to combat cybersecurity attacks. It creates greater productivity and cost savings for manufacturing to transportation and logistics and it leads to breakthroughs in health and medical research.

Innovation thrives in stable policy environments where new ideas can be explored and flourish within a well-understood legal and regulatory framework. So in December, Business Roundtable released a proposal for privacy legislation. Our proposal is the product of extensive deliberation with the chief privacy officers of our companies and approval from CEOs across industry sectors.

We believe that privacy legislation must prioritize four important objectives. First and foremost, it should champion consumer privacy and promote accountability. Legislation should include strong protections for personal data that enhance consumer trust and demonstrate U.S. leadership as a champion for privacy.

Second is fostering innovation and competitiveness especially in a dynamic and evolving technology landscape. Legislation should be technology-neutral and allow organizations to adopt privacy protections that are appropriate to the specific risks such as the sensitivity of the data.

Third, it should harmonize privacy protections. Congress should enact a comprehensive, national law that ensures consistent protections and avoids a State-by-State approach that leads to disjointed consumer protections, degraded user experience, and barriers to investment and innovation.

And fourth, legislation should promote consumer privacy regimes that are interoperable on a global basis and it should seek to bridge differences between the U.S. and foreign privacy regimes.

At the heart of the Business Roundtable proposal is a set of core individual rights that we believe consumers should have over their data, including transparency. Consumers deserve to have clear and concise understanding of the personal data that a company collects, the purposes for which that data is used, and whether and for what purposes personal data is disclosed to third parties.

Control, consumers should have meaningful control over their data based upon the sensitivity of the information including the ability to control whether that data is sold to third parties. Consumers should also have the right to access and correct inaccuracies in their personal data about them and they should have the right to delete personal data.

A Federal privacy law should be comprehensive and apply a consistent, uniform framework to the collection, use, and sharing of data across industry sectors. It should also recognize that there are situations that do justify exceptions such as cases of public health and safety, or to prevent fraud and provide cybersecurity, or when certain data is necessary to deliver a product or a service that the consumer requested, or to ensure First Amendment rights and to protect the rights of other individuals.

Establishing and protecting these consumer rights also requires effective, consistent, and coordinated enforcement to provide accountability and protect consumer rights. Absent action from Congress, we will be subject not only to a growing confusing set of State government requirements, but also to different data protection laws from governments in Europe, countries like Brazil, and elsewhere. Make no mistake, consumers deserve meaningful, understandable, and consistent privacy rights regardless of where they live and where their data may be located.

I thank the subcommittee for its leadership in holding this hearing and for encouraging a dialogue and I look forward to the questions. Thank you.

[The prepared statement of Ms. Zheng follows:]



Testimony of Denise E. Zheng
Vice President, Technology and Innovation, Business Roundtable

Before the House Energy and Commerce Subcommittee on Consumer Protection and Commerce

On "Protecting Consumer Privacy in the Era of Big Data"

February 26, 2019

Chairwoman Schakowsky, Ranking Member McMorris Rogers, Members of the Subcommittee, thank you for the opportunity to testify. My name is Denise Zheng, and I serve as the vice president for technology and innovation at Business Roundtable, which represents more than 200 Chief Executive Officers (CEOs) of the largest American companies from all sectors of the economy including technology, telecommunications, retail, banking, health, manufacturing, energy, hospitality, insurance, transportation, automotive and other industries.

Business Roundtable companies operate in virtually every corner of the U.S. economy and touch virtually every American consumer. Our companies process more than \$16 trillion in global consumer payments each year, service roughly 40 million utilities customers across the country and fly more than 250 million passengers to their destinations each year. Business Roundtable companies provide wireless communications and internet services to more than 160 million consumers, sponsor nearly 70 million medical insurance memberships and deliver more than 42 million packages every single day.

Data privacy is a major priority for our member companies, especially as every company relies on data and digital platforms to deliver products and services to consumers and conduct day-to-day business operations. That is why Business Roundtable CEOs from across industry sectors have come together to call for a federal law that provides a consistent set of consumer privacy protections, promotes accountability, and fosters innovation and competitiveness.

Business Roundtable member companies strongly support giving consumers control over how their personally identifiable information is collected, used and shared. At the same time, it is important to remember the value of data in our economy, as well as the enormous benefits that data-driven services provide to consumers. Data enable companies to deliver more relevant and valuable user experiences to consumers. They enable companies to detect and prevent fraud on user accounts and combat cyberattacks. They enable greater productivity and cost-savings from manufacturing to transportation and logistics. They enable breakthroughs in health and medical research.

Talk to any economist, and he or she will tell you that innovation thrives in stable policy environments, where new ideas can be explored and flourish within a well-understood legal and regulatory framework. It is in fact because of our stable policy environment that the United States is the top global destination for developing and bringing to market innovative

technologies. But fragmentation of privacy regulation threatens to undermine that stable environment and is therefore a threat to innovation.

Federal privacy legislation should build on the strong foundation of U.S. privacy law and enforcement. Congress has enacted privacy laws focused on children and the health care and financial services industries, and the Federal Trade Commission has engaged in hundreds of privacy and data security enforcement actions as part of its consumer protection authority. However, there is no comprehensive federal consumer privacy law. In the absence of such a U.S. federal law, foreign governments — from Brussels to Brasilia to Beijing — and select U.S. states are creating inconsistent approaches to privacy both domestically and abroad. The result is a complex and difficult-to-navigate set of privacy regulations that creates inconsistent protections for consumers and undermines innovation in new technologies.

The issue of privacy is reaching a tipping point. Perhaps for the first time in the United States, there is widespread agreement among companies across all sectors of the economy, government and consumer groups of the need for a comprehensive federal consumer privacy law.

In December, Business Roundtable released a proposal for privacy legislation. The Business Roundtable proposal is the product of extensive deliberation with the Chief Privacy Officers of companies and has approval from CEOs across industry sectors.

Business Roundtable believes that federal privacy legislation must focus on the following important objectives as priorities:

- **Champion Consumer Privacy and Promote Accountability.** Legislation should include strong protections for personal data that enhance consumer trust and demonstrate U.S. leadership as a champion for privacy by including clear and comprehensive obligations regarding the collection, use and sharing of personal data as well as accountability measures to ensure that those obligations are met.
- **Foster Innovation and Competitiveness.** Legislation should be technology neutral and take a principles-based approach so organizations can adopt privacy protections that are appropriate to specific risks, such as the sensitivity of the data, as well as provide for continued innovation and economic competitiveness in a dynamic and constantly evolving technology landscape.
- **Harmonize Privacy Protections.** Legislation should eliminate fragmentation of privacy protections in the United States by harmonizing approaches to consumer privacy across federal and state jurisdictions through a comprehensive national law that ensures consistent privacy protections and avoids a state-by-state approach that leads to consumer confusion and makes compliance nationwide very challenging.

- **Achieve Global Interoperability.** Legislation also should facilitate international transfers of personal data and e-commerce. It should further promote consumer privacy regimes that are interoperable on a global basis, meaning the legislation should support consumer privacy while also respecting and bridging differences between U.S. and foreign privacy regimes.

At the heart of the Business Roundtable proposal is a set of core individual rights that we believe consumers should have over their data:

- The right to **transparency** regarding a company's data practices, including the types of personal data that a company collects, the purposes for which these data are used, and whether and for what purposes personal data are disclosed to third parties;
- The right to **exert control** over their data based upon the sensitivity of the information, including the ability to control whether their data are sold to third parties;
- The right to **access and correct** inaccuracies in personal data about them; and
- The right to **delete** personal data.

A federal privacy law should be comprehensive and apply a consistent, uniform framework to the collection, use and sharing of data across industry sectors. Such a law should also recognize that some situations justify exceptions, such as to address public health and safety concerns, prevent fraud and provide cybersecurity, deliver a product or service that the consumer requested, or ensure First Amendment rights and protect the rights of other individuals. Establishing and protecting these rights also requires consistent and coordinated enforcement to provide accountability and protect consumer privacy rights.

Absent action by Congress, U.S. companies will be subject not only to a growing, confusing set of state government requirements being made across the United States but also to different data protection laws from governments in Europe, countries such as Brazil and elsewhere. Make no mistake: A patchwork of confusing data privacy requirements does not benefit consumers, who deserve meaningful, understandable and consistent data privacy rights regardless of where they live or where their data may be located.

The United States must act now to establish a consistent national standard that eliminates fragmentation within our country's own borders, sets clear direction for companies, achieves some measure of global interoperability and gives consumers more control over their data.

Business Roundtable stands ready to work with Members of Congress as well as consumer protection advocates to support the development of federal privacy legislation that enhances privacy and accountability, fosters innovation, and harmonizes regulations within the United States.

Ms. SCHAKOWSKY. Thank you.

Mr. Grimaldi, you are now recognized for 5 minutes.

STATEMENT OF DAVID F. GRIMALDI, Jr.

Mr. GRIMALDI. Thank you, Chairman Schakowsky, Ranking Member McMorris Rodgers, and members of the committee. I appreciate the opportunity to testify here today. I am Dave Grimaldi, executive vice president for Public Policy at the Interactive Advertising Bureau which was founded in 1996 and headquartered in New York City. We represent over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns.

Today the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising also allows consumers to access these resources at little to no cost to them and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the internet's largest players.

As a result of this advertising based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a 2017 study, in 2016 the U.S. ad-supported internet created 10.4 million jobs and added 1.1 trillion to the U.S. economy.

The study, designed to provide a comprehensive review of the entire internet economy and answer questions about its size, what comprises it, and the economic and social benefits Americans derive from it, revealed key findings that analyze the economic importance as well as the social benefits of the internet. And, indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers would not be able to afford access to or would be reluctant to utilize all of the information, products, and services they rely on today and that could become available in the future.

The time is right for the creation of a new paradigm for data privacy in the United States. And IAB, working with Congress and based on our members' successful experience creating privacy programs that consumers understand and use, can achieve a new Federal approach that instead of bombarding consumers with notices and choices comprehensively describes clear, workable, and consistent standards that consumers, businesses, and law enforcers can rely upon. Without a consistent Federal privacy standard, a patchwork of State privacy laws will create consumer confusion, present substantial challenges for businesses trying to comply with these laws, and fail to meet consumers' expectations about their digital privacy.

We ask Congress to standardize privacy protections across the country by passing legislation that provides important protections for consumers while allowing digital innovation to continue to flourish. We caution Congress not to rely on the framework set forth in Europe's General Data Privacy Regulation or California's

Consumer Privacy Act as examples of the ways in which a national privacy standard should function.

Far from being a desirable model, the GDPR shows how overly restrictive frameworks can be harmful to competition and consumers alike. Less than a year into GDPR's applicability the negative effects of its approach have already become clear. The GDPR has led directly to consumers losing access to online resources with more than 1,000 U.S.-based publishers blocking European consumers from access to online material, in part because of the inability to profitably run advertising.

To that unfortunate end, as was pointed out before, I would note that the Chicago Tribune, including its Pulitzer Prize-winning stories on government corruption, faulty government regulation, et cetera, is no longer accessible in Europe due to GDPR. Additionally, the San Fernando Sun newspaper, which has been open since 1904, is no longer accessible, and The Holland Sentinel, founded in 1896, can no longer be seen in Europe.

Small businesses and startups also saw the negative impact of GDPR with many choosing to exit the market. Consent banners and pop-up notices have been notably ineffective at curbing irresponsible data practices or truly furthering consumer awareness and choice. The CCPA follows in the footsteps of GDPR and could harm consumers by impeding their access to expected tools, content, and services, and revealing their personal information to unintended recipients due to lack of clarity in the law.

To achieve these goals, IAB asks Congress to support a new paradigm that would follow certain 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. Consumers will then be protected from such practices without the need for any action on their part.

Second, a new law 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. And finally, the law should incentivize strong and enforceable compliance and self-regulatory programs and thus increase compliance by creating a rigorous safe harbor process.

IAB asks for Congress' support in developing such a framework. We look forward to partnering with you to enhance consumer privacy and thank you for your time today and I welcome your questions.

[The prepared statement of Mr. Grimaldi follows:]

BEFORE THE

HOUSE OF REPRESENTATIVES SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE
OF THE COMMITTEE ON ENERGY AND COMMERCE

HEARING ON

PROTECTING CONSUMER PRIVACY IN THE ERA OF BIG DATA

FEBRUARY 26, 2019

TESTIMONY OF

DAVID F. GRIMALDI, JR.

EXECUTIVE VICE PRESIDENT, PUBLIC POLICY

INTERACTIVE ADVERTISING BUREAU

Chairwoman Schakowsky, Ranking Member Rodgers, and Members of the Committee, thank you for the opportunity to testify today. I am Dave Grimaldi, Executive Vice President for Public Policy at the Interactive Advertising Bureau (“IAB”). Founded in 1996 and headquartered in New York City, the IAB represents over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns. Together, our members account for 86 percent of online advertising in the United States.

Working with our member companies, the IAB develops technical standards and best practices, conducts critical research on interactive advertising, and educates brands, agencies, and the wider business community on the importance of online marketing to digital trade. I am honored to discuss with you today the important work that IAB and its members are engaged in to support consumer privacy while helping businesses of all sizes succeed online. We believe the time is right for a new, federal paradigm on consumer privacy that sets 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. This is a critical moment for Congress to step in and prevent the country from ending up with a patchwork of ambiguous and inconsistent state laws that will create uncertainty for business and uneven protections for consumers. We look forward to working with the Committee to set a national data standard that works for consumers and businesses alike.

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.¹ Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.² The study, designed to provide a comprehensive review of the entire Internet economy and answer questions about its size, what comprises it, and the economic and social benefits Americans derive from it, revealed key findings that analyze the economic importance, as well as the social benefits, of the Internet.

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to

¹ John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

² *Id.*

valuable content, or the ability to create their own platforms to reach millions of their fellow citizens. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the Federal Trade Commission (“FTC”) noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.³

II. IAB Members Have Long Supported Strong Consumer Privacy Protections

The IAB and its members have been at the forefront of promoting responsible data practices, and consumer trust is vital to our member companies’ ability to operate successfully in the marketplace. The Internet’s framework made customer relationships the core asset of every successful enterprise, and data is replacing legacy assets like a company’s manufacturing footprint or access to raw physical materials. The success of a business is premised on having personalized relationships with millions of consumers at scale, and that is best achieved only when companies responsibly use the information that customers have provided about themselves. Such data is the key driver of companies’ growth, ability to reach individuals at scale, and creation of consumer value in the modern digital age. Consumers expect and appreciate the

³ Federal Trade Commission, *In re Developing the Administration’s Approach to Consumer Privacy*, 15 (Nov. 13, 2018) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

tailored experiences that are possible using data. We strongly believe that businesses can address consumer concerns by preventing harmful and unexpected uses of data while preserving beneficial ones.

This commitment to consumer trust, and recognition that data is essential for business success, is best exemplified through IAB's integral role in the creation of the self-regulatory systems administrated by the Digital Advertising Alliance ("DAA"). The DAA is 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, based on practices recommended by the FTC in its 2009 report on online behavioral advertising.⁴ The rules set by the DAA have continued to evolve in the intervening years to account for new data practices.

Today, the DAA Principles provide consumer transparency and control regarding data collection and use of web viewing data, application use data, precise location data, and personal directory data.⁵ The DAA Principles also contain strong prohibitions on the use of such data for eligibility purposes for employment, insurance, credit, and healthcare treatment,⁶ and detailed guidance around the application of the Principles in the mobile⁷ and cross-device⁸ environments. Most recently, to provide users with increased transparency about the source of the political advertising they see online, the DAA released guidance on the application of the Principles of

⁴ DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009) <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>; FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>.


⁵ DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009) <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>; DAA, *Self-Regulatory Principles for Multi-Site Data (MSD)* (Nov. 2011) <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>; DAA, *Application of Self-Regulatory Principles to the Mobile Environment*, (Jul. 2013) http://www.aboutads.info/DAA_Mobile_Guidance.pdf.

⁶ DAA, MSD, 4-5 (Nov. 2011); DAA, *Application of Self-Regulatory Principles to the Mobile Environment*, 31-32 (Jul. 2013).

⁷ DAA, *Application of the Self-Regulatory Principles to the Mobile Environment* (Jul. 2013).

⁸ DAA, *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015).

transparency and accountability to political advertising.⁹ Importantly, the YourAdChoices Program and the DAA Principles are a novel kind of industry-led initiative whereby *all* companies engaging in the covered practices are subject to established privacy safeguard obligations. The DAA Principles are independently monitored and enforced by accountability programs. To date, more than 90 compliance actions have been publicly announced, and additional investigations have occurred without being made public.

One of the innovations of the DAA program has been the DAA's YourAdChoices Icon . This icon is served in or near ads over a trillion times per month worldwide in order to provide transparency outside of the privacy policy. By clicking this icon in any ad, consumers can see more information about interest-based advertising and can access simple, one-button tools to control the future collection and use of data for interest-based advertising. Consumer awareness and understanding of the program continues to increase, and a 2016 study showed more than three in five consumers (61 percent) recognized and understood what the YourAdChoices Icon represents.¹⁰

The effectiveness of the DAA Self-Regulatory Program also has been recognized by the United States government. At a 2012 White House event, Obama Administration officials including the then-FTC Chairman and then-Secretary of Commerce publicly praised the DAA's cross-industry initiative. The DAA's approach has also garnered kudos over time from the leadership at the FTC and from FTC staff for the program's pioneering privacy work.¹¹

⁹ DAA, *Application of Self-Regulatory Principles of Transparency & Accountability to Political Advertising*, (May 2018).

¹⁰ DAA, *Consumers' recognition of the AdChoices Icon -- and understanding of how it gives choice for ads based on their interests -- continues to rise* (Sep. 29, 2016) <https://digitaladvertisingalliance.org/blog/icon-you-see-yeah-you-know-me-0>.

¹¹ The White House recognized the Self-Regulatory Program as "an example of the value of industry leadership as a critical part of privacy protection going forward." The DAA also garnered kudos from then-Commissioner Maureen Ohlhausen who stated that the DAA "is one of the great success stories in the [privacy] space." In its cross-device tracking report, the FTC staff also

III. The Existing U.S. Privacy Framework Should be Updated

The time is right for the creation of a new paradigm for data privacy in the United States. IAB, working with Congress, and based on our members' successful experience creating privacy programs that consumers understand and use, can achieve a new federal approach that, instead of bombarding consumers with notices and choices, comprehensively describes clear, workable, and consistent standards that consumers, businesses, and law enforcers can rely upon. Without a consistent federal privacy standard, a patchwork of state privacy laws will create consumer confusion, present substantial challenges for businesses trying to comply with these laws, and fail to meet consumers' expectations about their digital privacy. We ask the Congress to standardize privacy protections across the country by passing legislation that provides important protections for consumers while allowing digital innovation to continue apace.

We caution Congress not to rely on the frameworks set forth in Europe's General Data Privacy Regulation ("GDPR") or California's Consumer Privacy Act ("CCPA") as examples of the ways in which a national privacy standard should function. These frameworks are not new approaches, only more restrictive versions of the existing privacy paradigm. While well-intentioned, their rigid frameworks impose significant burdens on consumers, such as rampant over-notification leading to consent fatigue in consumers and creating an indifference to important notices regarding their privacy. At the same time, these regimes fail to stop many practices that are truly harmful to consumers. These laws also display a misguided antagonism

praised the DAA for having "taken steps to keep up with evolving technologies and provide important guidance to [its] members and the public. [Its] work has improved the level of consumer protection in the marketplace."

toward online advertising, and fail to recognize the various ways in which digital advertising subsidizes the rich online content and services that consumers want.

Far from being a desirable model, the GDPR shows how overly restrictive frameworks can be harmful to competition and consumers alike. Less than a year into the GDPR's applicability, the negative effects of its approach have already become clear. Following the GDPR's enforcement date, the volume of programmatic advertising in Europe dropped between 25 and 40 percent across exchanges.¹² The GDPR has also directly led to consumers losing access to online resources, with more than 1,000 U.S.-based publishers blocking European consumers from access to online material in part because of the inability to profitably run advertising.¹³ At least one major U.S. newspaper is charging European subscribers an additional \$30 to access its online content because of an inability to run effective and profitable advertising in that market.¹⁴

Small businesses and startups also saw the negative impact of the GDPR, with many choosing to exit the market. Prior to the GDPR's enforcement date, according to media reports, some smaller companies in the United States chose to leave the European market instead of risk the fines related to potential GDPR violations.¹⁵ Over the time the GDPR has been in effect, some academic research estimates that startup investments in European companies have dropped

¹² Jessica Davies, DigiDay, *GDPR mayhem: Programmatic ad buying plummets in Europe* (May 25, 2018) <https://digiday.com/media/gdpr-mayhem-programmatic-ad-buying-plummets-europe/>.

¹³ 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/>.

¹⁴ 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/>.

¹⁵ Ivana Kottasová, CNNBusiness, *These companies are getting killed by GDPR* (May 11, 2018) <https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html>; Hannah Kuchler, *Financial Times*, *US small businesses drop EU customers over new data rule* (May 24, 2018) <https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04>.

40 percent in aggregate.¹⁶ These examples show the clear imbalance that the GDPR strikes between innovation and privacy.

The GDPR and CCPA fail to achieve their stated goals in a multitude of ways. The GDPR, for example, places inflexible requirements on businesses in the name of consumer privacy, but falls short of giving consumers real and effective rights and choices. Consent banners and pop-up notices have been notably ineffective at curbing irresponsible data practices or truly furthering consumer awareness and choice. The CCPA follows in the footsteps of the GDPR and could harm consumers by impeding their access to expected tools, content, and services; revealing their personal information to unintended recipients due to the lack of clarity in the law; and allowing unregulated third parties to access personal information under 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 refrain from doing business in California altogether – a move that some companies have already taken in Europe in response to the GDPR. 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.

Congress should look to a new paradigm for digital privacy that will not threaten the goods and services that consumers seek on the Internet. Consumers rely on the ad-supported model to enjoy the Internet's free content and services. Consumers understand and support the exchange of value in which data-driven advertising funds the free or reduced cost online services

¹⁶Mark Scott *et al.*, *Six months in, Europe's privacy revolution favors Google, Facebook* (Nov. 23, 2018) <https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/>.

they receive. In fact, a DAA-commissioned Zogby survey found that consumers attributed a value of nearly \$1,200 a year to common online ad-supported services, like news, weather, video content, and social media.¹⁷ A large majority of surveyed consumers (85 percent) like the ad-supported model, and 75 percent said they would greatly decrease their use of the Internet were they required to pay hundreds of dollars a year for currently free content.¹⁸ The new federal privacy standard should take into account the fact that consumers overwhelmingly value and want to keep their access to ad-supported online resources.

An effective new paradigm also should shift the burden of privacy compliance away from consumers. Consumers want to know their privacy is protected, but they cannot spend hours every day finding, reading, and interpreting privacy notices, as regimes like the GDPR and CCPA envision. Instead, Congress should develop clear rules that describe which data practices are permitted and prohibited. Just as when rules for automobile safety were developed, consumers should be able to look to Congress to create reasonable, responsible, and sensible standards to protect their privacy in a smart way.

To achieve these goals, the IAB asks Congress to support a new paradigm that would follow certain 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. Consumers will then be protected from such practices without the need for any action on their part. Second, a new law should distinguish between data practices that pose a threat to consumers and those that do not, rather than taking a broad-brush

¹⁷ Zogby Analytics, *Public Opinion Survey On Value Of The Ad-Supported Internet* (May 2016) https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.

¹⁸ *Id.*

approach to all data collection and use. Third, the law should incentivize strong and enforceable compliance and self-regulatory programs, and thus increase 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’s support in developing such a framework to enhance consumer privacy. Thank you for your time today. I welcome your questions.

* * *

Ms. SCHAKOWSKY. Thank you.

And, Ms. O'Connor, you are recognized for 5 minutes.

STATEMENT OF NUALA O'CONNOR

Ms. O'CONNOR. Chairwoman Schakowsky, Ranking Member McMorris Rodgers, members of the subcommittee, thank you for the opportunity to testify today. My colleagues and I at the Center for Democracy & Technology are tremendously excited about the prospect of Federal privacy legislation. We appreciate your leadership in taking on this challenging issue.

Privacy and data over the last several decades have become full of jargon and overly complexified, so I have one basic message today and that is notice and choice are no longer a choice. Any privacy legislation that merely cements the current status quo of the notice and consent model for personal data is a missed opportunity.

Let me take a moment to demonstrate why that status quo is not working for individual consumers and companies. If I could respectfully request the Members and their staff to take out their phones—some of you already have them out, I hear them ringing—and take a look at the home page. Open it up with whatever you use to open up your phone. Mine is my fingerprint and it is not working. Now look at your home page. How many apps do you have? I have 262 apps on my phone. I had 261 until Saturday night when the kids said, “Mom, we want Chipotle for dinner,” and I had to download again the Postmates app, so now it is 262. The average person has around 80, according to current research. You can call me an overachiever or just a working mom.

But for each of these 80 or so applications you have already given the company behind it your consent to use your personal data and likely in a variety of ways. For some of those apps you are sharing your location data, others your financial data, your credit card numbers, some of your apps have information about your physical activity, your health, and other intimate information even in real time.

Regardless of the types of data, you have received 80 notices and 80 different consents have already been given. Do you remember the personal data you agreed to consent to give and do you remember the purposes for which you shared it? Do you have a good understanding of how the companies behind those apps and devices are going to use that information 6 weeks from now, 6 months or 6 years from now?

Now let's assume for the sake of this demonstration that each of those 80 companies has even just a modest number of information-sharing agreements with third parties. Back in 2015, which is the ancient times of the internet, the average smart phone app was already automatically sharing data with at least three companies and three different parties. You don't know those companies, you don't have a direct relationship with them, and now they have your personal information because you were given notice and you consented. And that means the average smart phone user has given consent for their data to be used by at least 240 different entities.

That doesn't reflect how information is already being shared by the companies with vendors, corporate affiliates, business partners—in reality, the number is likely much higher and that is just

what is on your phone. That 240 number doesn't account for your other devices, the devices in your daily life in your house, in your car, your other online accounts, data initially collected in the non-digital world, loyalty programs, cameras, paper surveys, and public records. Does that feel like you have control over your personal information? But you gave your consent at some point.

Clearly, it is time for a change. Some will say that the way to fix this problem is just make more privacy policies, more notices, make them clearer so consumers can better understand those decisions. More checkboxes will provide the appearance of choice, but not real options for consumers. Pursuing legislation like this just doubles down on our current system of notice and choice and further burdens already busy consumers.

There is fundamentally no meaningful way for people to make informed, timely decisions about the many different data collectors and processors with whom we interact every day. Instead, the goal should be to define our digital civil rights. What reasonable behavior can we expect from companies that hold our data? What rights do we have that are so precious they cannot be signed away?

The Center for Democracy & Technology has drafted comprehensive legislation that is already available and has been shared with your staffs. I am happy to answer questions about it today. But most importantly, our bill and any meaningful privacy legislation must first prohibit unfair data practices, particularly the repurposing or secondary use of sensitive data with carefully scoped exceptions.

Two, prevent data-driven discrimination and civil rights abuses. Three, provide robust and rigorous enforcement. Reasonable data security practices and individual-controlled rights, such as the right to access, correct, and delete your data are obviously essential. Enacting clear comprehensive rules will facilitate trust and cement America's economic and ethical leadership on technology.

Now is the time for real change. You have the opportunity to shape a new paradigm for data use and you have the support of the majority of Americans to do so. Thank you.

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



**Statement of Nuala O'Connor, President and CEO
Center for Democracy & Technology**

**before the
United States House of Representatives Subcommittee on Consumer Protection and
Commerce of the Committee on Energy and Commerce
Protecting Consumer Privacy in the Era of Big Data**

February 26, 2019

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to testify about the imminent need for a foundational federal consumer privacy law. CDT is a nonpartisan, nonprofit 501(c)(3) charitable organization dedicated to advancing the rights of the individual in the digital world. CDT is committed to protecting privacy as a fundamental human and civil right and as a necessity for securing other rights such as access to justice, equal protection, and freedom of expression. CDT has offices in Washington, D.C., and Brussels, and has a diverse funding portfolio from foundation grants, corporate donations, and individual donations.¹

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

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

Department of Homeland Security under Secretary Tom Ridge, I was the first statutorily mandated CPO in the federal service.

In my testimony before the Senate Committee on Commerce, Science, and Transportation in October, I said that it was time to acknowledge the impacts of ubiquitous data collection and sharing, and to pass clear rules that would provide certainty to both companies and consumers.² In the months since that hearing, the urgency for Congress to pass strong and comprehensive privacy protections has mounted. New investigative reporting has revealed an unbounded secondary market for Americans' sensitive information, such as location³ and health data.⁴ Data brokers continue to build secretive and detailed profiles that can be used to exploit or discriminate based on race, religion, gender, age, and other protected categories.⁵ Consumers have made it clear that they want certainty, not surprises, when they entrust their personal information to a company. It's time for Congress to deliver the privacy protections we have been waiting for.

CDT's vision for our digital future is one in which technology supports human rights and human dignity. This future cannot be realized if people are forced to choose between protecting their personal information and using the technologies and services that enhance our lives. This future depends on clear and meaningful rules governing data processing; rules that do not simply provide people with notices and check boxes but actually protect them from privacy and security abuses and data-driven discrimination; protections that cannot be signed away.

We understand that drafting comprehensive privacy legislation is a complex endeavor. Over the past year we have worked with partners in civil society, academia, and various industry sectors to produce draft legislation that is both meaningful and workable. This testimony will discuss the components of our draft and why they should be incorporated into a federal privacy law.

² Statement of Nuala O'Connor, President & CEO, Ctr. for Democracy & Tech., before S. Comm. Commerce, Science & Transportation (Oct. 10, 2018), <https://cdt.org/insight/nuala-oconnors-written-testimony-before-senate-commerce-consumer-data-privacy-hearing/>.

³ See Jennifer Valentino DeVries et al., *Your apps know where you were last night, and they're not keeping it a secret*, N.Y. Times (Dec. 10, 2018), <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>.

⁴ Derek Kravitz & Marshall Allen, *Your medical devices are not keeping your health data to themselves*, Pro Publica (Nov. 21, 2018), <https://www.propublica.org/article/your-medical-devices-are-not-keeping-your-health-data-to-themselves>.

⁵ Yael Grauer, *Here's a long list of data broker sites and how to opt-out of them*, Motherboard (March 27, 2018), https://motherboard.vice.com/en_us/article/ne9b3z/how-to-get-off-data-broker-and-people-search-sites-pi-pl-spokeo.

Privacy legislation must (1) provide individual rights to access, correct, delete, and port personal information; (2) require reasonable data security and corporate responsibility; (3) prohibit unfair data practices, particularly the repurposing or secondary use of sensitive data, with carefully scoped exceptions; (4) prevent data-driven discrimination and civil rights abuses; and (5) provide robust and rigorous enforcement, including additional personnel and original fining authority for the Federal Trade Commission (FTC). The future of this country's technology leadership depends on this Congress passing clear, comprehensive rules of the road that facilitate trust between consumers and the organizations that collect and use their data.

The Need for Federal Legislation

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

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

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

- A New York Times investigation found that many of the apps that collect location information for localized news, weather, and other location services repurpose or share that information with third parties for advertising and other purposes. The investigation also suggested that users believe they are sharing location data for a specific location-based service, not giving free rein for any use sharing.⁶

⁶ DeVries, *supra* note 3.

- A Congressional investigation found that location data sold to third parties by internet service providers (ISPs) was used by prison officials to track innocent Americans.⁷ A Motherboard investigation found that bounty hunters could also access detailed location data sold by ISPs.⁸
- General Motors bragged in September that the company had secretly gathered data on driver's radio-listening habits and where they were when listening "just because [they] could."⁹ This data was exfiltrated from cars using built-in WiFi, which consumers can only use if they agree to GM's terms of service.
- Madison Square Garden deployed facial recognition technology purportedly for security purposes, while vendors and team representatives said the system was most useful for customer engagement and marketing.¹⁰
- Application developer Alphonso created over 200 games, including ones targeted at children, that turn on a phone's microphone solely for marketing purposes.¹¹
- Facebook permitted housing advertisements to be obscured from parents, disabled people, and other groups protected by civil rights laws.¹²

While the Federal Trade Commission's ability to police unfair and deceptive practices provide a backstop, large gaps in policies around access, security, and privacy exist, which confuse both individual consumers and businesses. Because the FTC is prohibited from using traditional rulemaking processes, the agency has developed a "common law" of privacy and security through its enforcement actions.¹³ Creating proactive privacy rights through an episodic approach will not be able to keep up with advances in technology and the explosion of device and app manufacturers.

Moving Beyond Notice and Consent

⁷ See ltr from Sen. Ron Wyden to Randall L. Stephenson, President and CEO, AT&T (May 8, 2018), <https://www.documentcloud.org/documents/4457319-Wyden-Securus-Location-Tracking-Letter-to-AT-am-p-T.html>.

⁸ Joseph Cox, *I gave a bounty hunter \$300. Then he located our phone*, Motherboard (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-mic-robilt-zumigo-tmobile.

⁹ Cory Doctorow, Every minute for three months, GM secretly gathered data on 90,000 drivers' radio-listening habits and locations, BoingBoing (Oct. 23, 2018), <https://boingboing.net/2018/10/23/dont-touch-that-dial.html>.

¹⁰ Kevin Draper, Madison Square Garden Has Used Face-Scanning Technology on Customers, NYT, Mar. 13, 2018.

¹¹ Sapna Maheshwari, That Game on Your Phone May Be Tracking What You Watch on TV, NYT, Dec. 28, 2017, <https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html>.

¹² Braktkon Booker, HUD Hits Facebook for Allowing Housing Discrimination, NPR, Aug. 19, 2018, <https://www.npr.org/2018/08/19/640002304/hud-hits-facebook-for-allowing-housing-discrimination>.

¹³ Daniel Solove and Woody Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia L. Rev. 583, (2014).

Existing privacy regimes rely too heavily on the concept of notice and consent, placing an untenable burden on consumers and failing to rein in harmful data practices.¹⁴ These frameworks simply require companies to provide notice of their data practices and get some kind of consent—whether implied or express—or provide users with an array of options and settings. This model encourages companies to write permissive privacy policies and entice users to agree to data collection and use by checking (or not unchecking) a box.

This status quo burdens individuals with navigating every notice, data policy, and setting, trying to make informed choices that align with their personal privacy interests. The sheer number of privacy policies, notices, and settings or opt-outs one would have to navigate is far beyond individuals' cognitive and temporal limitations. It is one thing to ask an individual to manage the privacy settings on their mobile phone; it is another to tell them they must do the same management for each application, social network, and connected device they use. Dozens of different data brokers operate different opt-outs.¹⁵ Further, people operate under woefully incorrect assumptions about how their privacy is protected.¹⁶ Privacy self-management alone is neither scalable nor practical for the individual. Burdening individuals with more and more granular decisions, absent some reasonable boundaries, will not provide the systemic changes we need.¹⁷

Moreover, people can be harmed by data processors with whom they have no direct relationship, making control impossible. Last year, for example, the fitness tracking app Strava displayed a heatmap of users' runs that revealed the locations and outlines of military and covert activity that could be used to identify interesting individuals, and track them to other sensitive or secretive locations.¹⁸ The harms stemming from this type of disclosure can reach people who never used the app and thus never had the option to consent to Strava's data policies.

¹⁴ See, e.g., Fred Cate, The Failure of Fair Information Practice Principles, in *THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES* 342, 351 (Jane Winn ed., 2006); and Solon Barocas & Helen Nissenbaum, On Notice: The Trouble with Notice and Consent, *Proceedings of the Engaging Data Forum*, (2009).

¹⁵ Grauer, *supra* note 5.

¹⁶ Joseph Turow, Let's Retire the Phrase 'Privacy Policy', *N.Y. Times* (Aug. 20, 2018), <https://www.nytimes.com/2018/08/20/opinion/20Turow.html>.

¹⁷ Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 *Harv. L. Rev.* 1880 (2013); Aleecia McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 *I/S: A Journal of Law and Policy* 543, (2008); Joel Reidenberg, Presentation, Putting Disclosures to the Test (2016), available at <https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test>.

¹⁸ Jeremy Hsu, The Strava Heatmap and the End of Secrets, *Wired*, Jan. 29, 2018, <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/>.

Even if an individual wants to make informed decisions about the collection, use, and sharing of their data, user interfaces can be designed to tip the scales in favor of disclosing more personal information. For example, the FTC reached a settlement with PayPal in February after its Venmo service misled users about the extent to which they could control the privacy of their financial transactions.¹⁹ Users' transactions could be displayed on Venmo's public feed even if users set their default audience to private. In the case of the Cambridge Analytica disclosure, users purportedly consented to disclosing information by filling out a quiz, but had no way of foreseeing how that information would be used.²⁰

Another weakness of notice-and-choice models is their inability to address discriminatory uses of data. Commercial data can be used in ways that systematically discriminate based on minority or protected classes such as race, age, gender, sexual orientation, disability, or economic status. Data-driven discrimination is inherently difficult for individuals to detect and avoid, and cannot be solved with a check box.

CDT is not the only entity to critique notice and consent as the predominant privacy control in U.S. law. The National Telecommunications and Information Administration (NTIA) acknowledged the shortcomings of the notice-and-consent model. The administration's request for comment on privacy noted that "relying on user intervention may be insufficient to manage privacy risks."²¹ Of course, constructing a new framework is complicated and will only happen by way of statute. It is time to rebuild that trust by providing a baseline of protection for Americans' personal information that is uniform across sectors, that follows the data as it changes hands, and that places clear limits on the collection and use of personal information.

What Legislation Should Include

Instead of relying primarily on privacy policies and other transparency mechanisms, Congress should pass explicit and targeted privacy protections for consumer data. As discussed below, legislation should (1) provide individual rights to access, correct, delete, and port personal information; (2) require reasonable data security and corporate responsibility; (3) prohibit unfair data practices, particularly the repurposing or secondary use of sensitive data,

¹⁹ Press release, FTC, Feb. 28, 2018, <https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information>.

²⁰ Kevin Granville, Facebook and Cambridge Analytica: What you Need to Know as Fallout Widens, NYT, Mar. 19, 2018, <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>.

²¹ National Telecommunications and Information Administration, Request for Comments on Developing the Administration's Approach to Consumer Privacy, Sept. 25, 2018, <https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy>.

with carefully scoped exceptions; (4) prevent data-driven discrimination and civil rights abuses; and (5) provide a robust and fair enforcement mechanism including original fining authority for the FTC.²²

Individual Rights in Data

A federal law must include basic rights for individuals to access, correct, delete, and port their personal data.²³ CDT's draft legislation would provide broad access and deletion rights, with tailored exceptions to account for technical feasibility, legitimate needs such as fraud detection and public interest research, and free expression rights. It also provides a right to dispute the accuracy and completion of information used to make critical decisions about a person, such as eligibility for credit, insurance, housing, employment, or educational opportunities. No one should be subject to life-altering decisions based on inaccurate or incomplete data. The draft also includes a right to transfer one's data from one service to another, where technically feasible (known as "data portability").

These rights would apply not only to information directly disclosed to a covered entity but also to information inferred by the covered entity, since inferences can often be more sensitive and opaque to users (e.g., inferring a medical condition based on someone's non-medical purchase history). A 2013 report from the Senate Commerce Committee found that data brokers created and sold consumer profiles identifying people as "Rural and Barely Making It," "Ethnic Second-City Strugglers," and "Retiring on Empty: Singles."²⁴ This information can be used to target vulnerable consumers with potentially harmful offers, such as payday loans.²⁵

A federal law must also enshrine the right to know how and with whom personal data is shared. Our draft requires disclosure of the names of third parties with whom information is shared. Some models only require disclosure of the categories of entities with whom data is

²² While we do not address transparency per se in this statement, we assume that any legislation will include such provisions and are available to discuss possibilities in detail with Congressional offices.

²³ Rob Pegoraro, *Web companies should make it easier to make your data portable: FTC's McSweeney*, USA Today (Nov. 12, 2017), <https://eu.usatoday.com/story/tech/columnist/2017/11/12/web-companies-should-make-easier-make-your-data-portable-ftcs-mcsweeney/856814001/>.

²⁴ Staff Report, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, S. Committee on Commerce, Science & Transportation (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

²⁵ See, e.g., Upturn, *Led Astray: Online Lead Generation and Payday Loans* (Oct. 2015), https://www.upturn.org/static/reports/2015/led-astray/files/Upturn_-_Led_Astray_v.1.01.pdf.

shared, which tells consumers and regulators very little about where the data is going and how it's being used.

These overarching rights are relatively noncontroversial. Companies must already extend them to their EU users under the General Data Protection Regulation (GDPR), and elements of these rights are also at the core of the California Consumer Privacy Act. They have been recognized by the U.S. government and international bodies for decades, albeit in voluntary form.²⁶ With appropriate, tailored exceptions, these provisions can be crafted in a way that does not unduly burden companies' business practices or interfere with the provision of services.

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

Affirmative Obligations to Protect Data

Entities that collect, use, and share data have a responsibility to safeguard it and prevent misuse. CDT's draft legislation would require covered entities to adopt reasonable data security practices and engage in reasonable oversight of third parties with whom they share personal information. These obligations recognize the reality that participating in modern society often means ceding control of one's personal information. The entities we trust with our data should handle it with care.

Our draft would also require covered entities to publish detailed disclosures of their data practices in a standardized, machine readable format that can be scrutinized by regulators and advocates. This annual report would be in addition to the real time disclosures made to users at the time they sign up for a new service or activate a device, or the privacy policies that operate at any one time. Ideally, these reports will result in detailed and standardized accounts of data processing that can be used by regulators, advocates, and privacy researchers to scrutinize covered entities on behalf of consumers.

Like individual rights, data security and standardized notices should be relatively non-controversial, but they are not enough to protect privacy. Proposals that include only access/correction/deletion rights and transparency, without meaningful limits on the collection and use of data, are insufficient.

²⁶ Robert Gellman, *Fair Information Practices: A History*, 2012, <https://bobbegelman.com/rg-docs/rg-FIPshistory.pdf>.

Prohibiting Unfair Data Practices

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

While data provided in the context of a commercial transaction can often be considered part of an ongoing business relationship, and used in the context of future transactions between the parties, there are some types of data and some processing practices that are so sensitive that they should be permitted only to provide a user the service they requested, and prohibited from entering the opaque and unaccountable market of secondary uses. CDT's draft would prohibit the following data processing practices, with some exceptions, when the processing is not required to provide or add to the functionality of a service or feature that the user has affirmatively requested:

- The processing of biometric information to identify a person;
- The processing of precise geolocation information;
- The processing of health information;
- The use of children's information for targeted advertising and disclosure to third parties;
- The licensing or sale to third parties of the contents of communications or the parties to a communication (such as call or email logs);
- The retention, use, or disclosure of audio and visual recordings; and
- The use of probabilistic inferences to tracking people across different devices.

These categories involve information that is particularly sensitive and types of processing or repurposing that are typically unexpected and difficult to foresee. If a user downloads a mapping service and agrees to provide precise location information, that information should only be used to provide and improve the performance of that service and not, for example, to provide data to retailers about the user's proximity to their stores. These guardrails would provide certainty to companies while allowing them to provide valuable data-driven services, and would allow users to share sensitive data with reasonable expectations that it will be safeguarded. Technology changes quickly and it can be difficult for the law to keep pace, so we have also drafted a safety valve whereby companies can petition the FTC to create specific exceptions to these prohibitions. Our bill also includes narrowly scoped exceptions for data security and fraud prevention and emergencies.

Preventing data-driven discrimination

In its 2016 Big Data report, the Federal Trade Commission (FTC) found that “big data offers companies the opportunity to facilitate inclusion or exclusion.” Unchecked data processing and algorithmic decisionmaking can amplify discrimination based on race, gender, sexual orientation, ability, age, financial status, and other group membership. Since the FTC’s report, discriminatory data practices have continued, but little has been done to address them. CDT and 42 other organizations wrote in a letter to Congress that any federal privacy legislation must address data-driven discrimination.²⁷ The letter states:

Civil rights protections have existed in brick-and-mortar commerce for decades. It is time to ensure they apply to the internet economy as well. Platforms and other online services should not be permitted to use consumer data to discriminate against protected classes or deny them opportunities in commerce, housing, and employment, or full participation in our democracy.²⁸

The data economy offers new opportunities to target information and personalize experiences, but it also creates new opportunities for exclusion based on protected group membership and for exploitative targeting.

- Journalists and researchers have demonstrated how advertising platforms can be used to target housing, job, and credit ads away from protected classes (e.g., excluding categories like “mothers” or “wheelchair users” from seeing a housing ad). Targeting affects who gets to learn about and apply for an opportunity.²⁹

²⁷ Ltr from 43 organizations to members of Congress, Address data-driven discrimination, protect civil rights (Feb. 13, 2019), <http://civilrightsdocs.info/pdf/policy/letters/2019/Roundtable-Letter-on-CRBig-Data-Privacy.pdf>.

²⁸ *Id.*

²⁹ See Till Speicher et al., Potential for Discrimination in Online Targeted Advertising, *Proceedings of Machine Learning Research* 81:1–15, 8, T. 2 (2018), <http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf>; Julia Angwin and Terry Parris Jr., Facebook Lets Advertisers Exclude Users by Race, *ProPublica* (Oct. 28, 2016), <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>; Julia Angwin, Ariana Tobin & Madeleine Varner, Facebook (Still) Letting Housing Advertisers Exclude Users by Race, *ProPublica* (Nov. 21, 2017), <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>; Amit Datta, Michael Carl Tschantz & Anupam Datta, Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination, in *Proceedings on Privacy Enhancing Technologies* (2015), <https://arxiv.org/abs/1408.6491>; Amit Datta et al., Discrimination in Online Advertising: A Multidisciplinary Inquiry, in *Proceedings of Machine Learning Research* 81:1–15, 3–7 (2018), <http://proceedings.mlr.press/v81/datta18a/datta18a.pdf>; Julia Angwin, et. al, Dozens of Companies are

- Employers often rely on services that proactively match them with job candidates, but if those algorithms are based on past hiring preferences, they can replicate discriminatory patterns.³⁰
- Predictive analytics used to target health interventions or set insurance rates may be less accurate for minority groups that have historically been excluded from research data.³¹
- Advertisers have leveraged data to target risky, undesirable, or even fraudulent opportunities based on sensitive characteristics.³² The data broker industry has aggregated information from disparate sources and used it to create marketing segments such as “urban scramble,” “diabetes interest,” and sexual assault survivors.³³
- The payday loan and for-profit college industries have used sensitive segments as well as deceptive data collection interfaces to generate leads.³⁴

CDT’s draft legislation would direct the FTC to promulgate rules addressing unfair advertising practices, particularly those that result in unlawful discrimination in violation of civil rights law.

Meaningful enforcement mechanisms

Affirmative individual rights and data collection and use restrictions may ultimately be meaningless absent strong enforcement. While we believe that the FTC has been effective as the country’s “top privacy cop,” it is also an agency that desperately needs more resources.

Using Facebook to Exclude Older Workers From Jobs, Dec. 20, 2017, <https://www.propublica.org/article/facebook-ads-age-discrimination-targeting>.

³⁰ Miranda Bogen & Aaron Rieke, Help Wanted: An Examination of Hiring Algorithms, Equity, & Bias (Dec. 2018),

<https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf>.

³¹ See Kadja Ferryman & Mikaela Pitcan, Fairness in Precision Medicine (Feb. 2018), https://datasociety.net/wp-content/uploads/2018/02/Data.Society.Fairness.In_.Precision.Medicine.Feb2018.FINAL-2.26.18.pdf; Center for Democracy & Technology, Healgorithms: Understanding the Potential for Bias in mHealth Apps (Sept. 13, 2018),

<https://cdt.org/insight/healgorithms-understanding-the-potential-for-bias-in-mhealth-apps/>.

³² See, e.g., Upturn, *supra* note 25.

³³ Fed. Trade Comm’n, Data Brokers: A Call for Transparency & Accountability at v (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>; Pam Dixon, Statement before the Senate Committee on Commerce, Science and Transportation, Hearing on What Information Do Data Brokers Have on Consumers, and How Do They Use It? At 9, 12–13 (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/e290bd4e-66e4-42ad-94c5-fcd4f9987781/BF22BC3239AE8F1E971B5FB40FFEA8DD.dixon-testimony.pdf.

³⁴ Upturn, *supra* note 25.

Funding for the agency has fallen five percent since 2010, and its resources are strained.³⁵ In 2015, the FTC had only 57 full-time staff working in the Division of Privacy and Identity Protection, with additional staff working in enforcement and other areas that could touch on privacy.³⁶ In addition to more FTC funding, federal legislation must include two new statutory enforcement mechanisms.

First, the FTC must be given the ability to extract meaningful fines from companies that violate individuals' privacy. Because much of the Commission's existing privacy enforcement falls under Section 5 of the FTC Act, it does not possess original fining authority and companies are functionally afforded one free "bite at the apple" regardless of the intent or impact of a privacy practice.³⁷ At present, before a company may be fined for violating individuals' privacy, it must first agree to and be placed under a consent decree, and then subsequently violate that agreement.

Relying solely on consent-decree enforcement is inadequate to protect user privacy. The penalties for violating a decree may be so insignificant that they do not have the intended deterrent effect. For instance, when Google agreed to pay a \$22.5 million penalty for violating terms of its consent order in 2012, this was approximately five hours' worth of Google's revenue at the time.³⁸

Second, state attorneys general must be granted the authority to enforce the federal law on behalf of their citizens. State attorneys general have been enforcing their own state consumer privacy laws for decades, first under state unfair and deceptive practice laws and more recently under state statutes targeted at specific sectors or types of data.³⁹ Employing their expertise will be necessary for a new federal privacy law to work. A law with the scope CDT are proposing will bring large numbers of previously unregulated entities into a proactive regime of new privacy and security requirements. There will simply be no way for a single agency like the FTC to absorb this magnitude of new responsibilities.

³⁵ David McCabe, Mergers are spiking, but antitrust cop funding isn't, AXIOS, May 7, 2018, <https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486-4a08-ab57-d3535ae43b52.html>; see also https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/?utm_term=.c6c304221989.

³⁶ <https://www.ftc.gov/system/files/documents/reports/fy-2016-congressional-budget-justification/2016-cbj.pdf>.

³⁷ Dissenting Statement of Commissioner J. Thomas Rosch, In the Matter of Google Inc., FTC Docket No. C-4336 (Aug. 9, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googleroschstatement.pdf>.

³⁸ Id. Commissioner Rosch noted that a \$22.5 million fine "represents a de minimis amount of Google's profit or revenues."

³⁹ Danielle Keats Citron, The Privacy Policy Making of State Attorneys General, 92 Notre Dame L. Rev. 747 (2016), <https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4693&context=ndlr>.

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

Conclusion

The existing patchwork of privacy laws in the United States has not served Americans well, and as connected technologies become even more ubiquitous, our disjointed privacy approach will only lead to more unintended consequences and harms. We risk further ceding our leadership role on data-driven innovation if we do not act to pass comprehensive privacy legislation. Effective privacy legislation will shift the balance of power and autonomy back to individual consumers, while providing a more certain and stable regulatory landscape that can accelerate innovation in the future. The time is now to restore the digital dignity for all Americans. Congress must show its leadership and pass a comprehensive privacy law for this country.

Ms. SCHAKOWSKY. Thank you.

So we have now concluded our opening statements and we now will move to Member questions. Each Member will have 5 minutes to ask questions of our witnesses and I will start by recognizing myself for 5 minutes.

So this is a stack of, really, just some of the privacy policies of the websites, apps, stores, and other services I interacted with just yesterday and actually not all of yesterday. I haven't read them all. And I check the weather on my phone so I have a privacy policy for that app. I flew into town yesterday. I have the privacy policy for the airline and for the online travel.

In order to get onto the plane I had to go my phone. I used the app to book the flight. I went to the drugstore and used my loyalty card so I have that privacy policy. I checked the news online so I have a few privacy policies of a few of the newspaper sites that I visited. I watched TV. I went online. I used my cell phone. I have a privacy policy for my cable provider, my internet service provider, my cell phone manufacturer and the operating system, and that is still just some of them.

And at that point did I have the option to proceed—and I didn't have the option at any point to proceed without agreeing to the terms. And frankly I think like most consumers because I am anxious to actually get the job done, I agree. I agree. So this stack does not include each of their service providers or affiliates or the data broker that gets my information from them or a third party advertiser, advertising company or analytic company or whoever else is lurking unseen to me and unheard and unknown.

By the way, a lot of these policies are pretty vague about what they do with my data and who they share it with or sell it to. This is the limitation of the notice and consent system that we use right now. A person should not need to have an advanced law degree to avoid being taken advantage of. We need to find solutions that take the burden off the consumer and put some responsibilities on those who want our data.

So, Ms. Collins-Dexter, can you talk a little bit about some of the ways that our data is being used by consumers and then, Ms. O'Connor, if you could follow up.

Ms. COLLINS-DEXTER. Some of the ways in which our data is being used by consumers?

Ms. SCHAKOWSKY. We are talking about—oh no, being—I am sorry—how it is being used by companies. I am sorry.

Ms. COLLINS-DEXTER. Yes, it is being used in all sorts of a number of ways. And I think to your point earlier, I think even if we know our data is being used in a number of ways, even if we—black folks, I think a report was released last week that said black people are actually more likely to read the fine print before they sign onto things on the internet and have long believed that their information and data was being sold, and yet that hasn't made us particularly safer. We have still had to experience all sorts of ways in which our data is being used against us.

Even data points that feel innocuous can be used as sort of proxies for protected class. I offered some examples in the document that I shared with you. But another example comes from the insurance industry in the realm of car insurance, for example. Auto in-

insurance telematics devices collect what would be considered, quote unquote, non-sensitive data such as vehicle speed, the time of day someone is driving, the miles driven, the rates of acceleration and braking.

Those devices aren't collecting what we would consider sensitive data such as location and driver's identity, and yet that information is being used to like charge people higher rates for insurance. And it happens at that people most likely to be driving at night, most likely to be braking, all of these things are usually like working, lower-class people.

Ms. SCHAKOWSKY. If I could interrupt, and we will get more of that. But I want to see if Ms. O'Connor wants to add at least one thing to this.

Ms. COLLINS-DEXTER. Sure.

Ms. O'CONNOR. Thank you so much.

There is a primary purpose for data. When you give your data to a company to deliver that yellow sweater they need to know your name and address. That makes sense. There are secondary purposes in terms of business processing and activities that might be legitimate, where we feel in our draft legislation the secondary purpose for sensitive data, like, for example, the fingerprint I was using to open my phone, I want to be able to open my phone with that, I don't want that sensitive biometric data used for a secondary purpose by that company or by other companies.

So we would say there is a higher level of sensitivity around biometric data. Intimate or immutable information about you deserves a second, a higher level of care. And also there is sharing, obviously there is your data going from a first party to an entirely separate third party in the transaction that would lead to concern and those parties should be bound by the promises that first party made.

Ms. SCHAKOWSKY. Thank you. And now let me recognize our ranking member, Cathy McMorris Rodgers.

Mrs. RODGERS. Thank you, Madam Chair. I appreciate again everyone being here, and I do believe that there is bipartisan support to move forward so that we can ensure strong protection of personal data that will ensure that we are improving upon consumer trust and demonstrating U.S. leadership in privacy and innovation.

I am concerned about the patchwork of privacy and security laws that I see coming at the State level. And we are moving forward in Washington State, there is a debate going on as well as other States that are taking action that I believe are going to lead to higher cost and impact on consumers. It is actually going to increase their prices and reduce the options that consumers have.

I would like to start with Dr. Layton and just ask the question, do you think that it is important for one Federal privacy law to set that national standard and, if so, just explain some more why.

Dr. LAYTON. Thank you for the question. I was heartened to hear our panelists and our representatives agree that we do need a comprehensive Federal standard.

Because California is such a large economy, if it can go forward with its particular rules it can dictate the rules for the rest of America. We have talked a lot about rights here on this panel and all of Americans have rights and it isn't fair that one State gets to dictate for everyone else. We should certainly look at California

and learn from them, but it is, as I understand, a law that came together in 1 week and that was their choice about how they did it. So I certainly agree that we need a national standard.

Mrs. RODGERS. I would like to ask Mr. Grimaldi and Ms. Zheng if you also would address this question and if your members agree with the one national standard.

Mr. GRIMALDI. Thank you, Congresswoman, we do. But make no mistake, we are very much in favor of the concepts of transparency and accountability and choice which are the bedrocks of CCPA and the reason that Californians came together to rally behind a law and the merits in it.

But to echo what Dr. Layton said, that patchwork could have incredibly negative effects on the American internet economy because it will force compliance costs not just on California companies but on all companies in America. It will imbalance what the larger providers can pay for those compliance costs and to retrofit their systems and to get ready to field what will be likely a barrage of lawsuits and, quite honestly, just fewer users, meaning fewer advertising costs once the enforcement of CCPA goes into effect in January.

And that is not indicative of a good privacy policy that provides to consumers what they currently enjoy, their content, their news, their video, and everything else.

Ms. ZHENG. I also completely agree. Thank you for that question, Ranking Member McMorris Rodgers.

I think from the Business Roundtable perspective a national consumer privacy law should not mean that consumers get less protections than currently exist, but if we set the standard at an appropriate level it can mean that every American across this country has protections that they don't currently have. So when we developed our proposal we looked at the California law. We looked at GDPR. We looked at other State proposals and FTC authority and tried to take the best practices of each of these individual laws in developing our proposal.

Mrs. RODGERS. Great. And just as a follow-up, I think as we move forward we need to be very concerned about making sure that we are protecting individuals' privacy but also ensuring that we are not becoming too regulatory, that the regulations are not too complex and through the regulations actually helping, or like the largest actors can pay those costs but it will make it harder for our startups and our innovators to get into the marketplace.

Dr. Layton, would you just address what you have seen with GDPR to date as far as the impact on businesses or innovators?

Dr. LAYTON. Yes. Well, in the case of the European Union, you have a data protection authority in each State and you have a super regulator overseeing that. And when this has come into play there was no training, there was no funding to help the particular agencies to get up to speed. They are not all equipped with the same set of skills. Some regulators may have worked there their whole life, other ones may be new. They have a different set of expertise. So, and each country had its own particular rules. And this issue and question around how do they manage this going forward that even the framers of the GDPR themselves said it will be 2

years before we have a judgment because of the actual process and how long it takes and so on.

So in the minds of the Europeans that this was also an important what they see as a way to empower government that they are looking to place people in jobs. They expect that they were going to have 75,000 more bureaucrats working in these particular jobs to look over the privacy and so on. So it is—they are sort of—it reflects what is going on in the EU today is a desperation. There are many people dissatisfied with the European Union. You probably know about Brexit. And this is a way that the EU is trying to respond to demonstrate to constituents that the EU can do something and it is not, you know, in the U.S. we might say, well, let's make it better or innovate——

Ms. SCHAKOWSKY. If you could wrap up.

Dr. LAYTON. Yes. So that was my point. Thank you.

Mrs. RODGERS. Thank you. I will yield back.

My time is expired.

Ms. SCHAKOWSKY. Now the gentlelady from Florida, Kathy Castor.

Ms. CASTOR. Thank you. You know, Americans are increasingly fed up with the violation of their privacy by online companies. There is just simply a massive amount of data being collected on each and every person. And then when that data is used, misused without their permission, or there is a breach of their financial data or their health data, I mean that is, it is really outrageous we have let it get this far. And I think American consumers understand that this needs to be fixed.

So I want to thank Chairwoman Schakowsky for calling this hearing, and I look forward to working with her and the other Members on this committee to adopt strong privacy protections for American families and consumers.

Ms. O'Connor, help us assess the current state of Americans' online privacy protections. Let me know if you agree or disagree with these statements. Currently there is no general Federal law that requires online companies to have privacy policies or protect our privacy. Is that correct or not correct?

Ms. O'CONNOR. That is correct.

Ms. CASTOR. And there is no general Federal law that requires an online company to secure our personal information or notify a customer if his or her personal information has been stolen. Is that correct?

Ms. O'CONNOR. That is correct.

Ms. CASTOR. And the only way the Federal Trade Commission is able to examine companies that violate our privacy is through Section 5, unfair or deceptive acts or practices authority, which basically means that companies can do whatever they want with our data as long as they don't lie about what they are doing. Is that right?

Ms. O'CONNOR. That is correct.

Ms. CASTOR. So is it accurate to say that a bad online actor can collect all sorts of very personal information such as your location, your birthday, your messages, your biometric data, your Social Security Number, political leanings without your permission and sell

it to the highest bidder as long as they don't lie about what they are doing?

Ms. O'CONNOR. That is pretty accurate.

Ms. CASTOR. Well, that is outrageous. And I think that is why American consumers now have—there has been an awakening to what has been happening. They understand this now and they are demanding strong privacy protections.

One of the areas that concerns me the most, Ms. Collins, is the data that is collected on children. There is a bedrock Federal law, the Children's Online Privacy Protection Act, that is supposed to protect kids from data being gathered on them and being targeted, but it was signed into law over 20 years ago. And think about how much the internet has changed in 20 years, the apps that are available to kids, the toys that talk to them and gather data.

Do you agree that COPPA needs to be updated as well?

Ms. COLLINS-DEXTER. Yes, I do. Can I expand on that a little more?

Ms. CASTOR. Please. I noticed in your testimony you cited a Cal Berkeley study where they identified how many apps targeted to kids that are probably gathering their data. Could you go into that in greater detail?

Ms. COLLINS-DEXTER. Yes. Yes. So I mean, I think a general—COPPA is the only Federal internet privacy law on the books and beyond that I think it is a solid blueprint for what comprehensive privacy legislation could look like with an opt-in model and placing obligations on companies for adequate disclosure. But as you point out, it is 20 years old and, like the Civil Rights Act, it does not account for the digital economy we are immersed in today.

So as I mention, a Cal Berkeley study found that thousands upon thousands of children's apps currently available on Google Play violate COPPA. The fact that the market is flooded with data collection apps and devices targeted at kids like Echo Dot, CloudPets, Furby Connect, and others should alarm us. More than one-third of U.S. homes have a smart toy. And so it is really important for us to like really, you know, think of the implications of that as we look to modernize that legislation.

Ms. CASTOR. Because we kind of have an understanding now that online companies are building profiles on all of us with huge amounts of data. But they are doing this to our kids now, notwithstanding the fact that we have a Federal law that supposedly says you can't do this. Is that right?

Ms. COLLINS-DEXTER. That is correct.

Ms. CASTOR. Ms. O'Connor, I don't think the average American parent understands that the apps and the toys that are provided, you know, for their kids to have fun and play games are creating these shadow profiles. Is that accurate?

Ms. O'CONNOR. I work in technology and I have many, many children and I feel overwhelmed with the choices and the lack of transparency about not just their online environment, but as you point out correctly the devices in our daily lives, even the toys and what they can and cannot collect. And it doesn't necessarily matter that it is identifiable by name if it is targeting you based on your habits and preferences and choices that could close their world

view as opposed to open it up, which is what we would hope the internet would do.

Ms. CASTOR. Thank you very much. I yield back.

Ms. SCHAKOWSKY. I now recognize the ranking member of the full committee, Mr. Walden, for 5 minutes.

I am sorry? Oh, I am sorry. Was that wrong?

OK, let me recognize Mr. Upton for 5 minutes.

Mr. UPTON. Thank you, Madam Chair. It is a delight to be here. I know that Mr. Walden is at the other hearing. I think he intends to come back.

Ms. Zheng, I think that we all recognize that the elephant in the room is truly we can have a system that is 40 or 50 with States or we are going to have one standard. What is the perception from the number of companies that you represent from the Business Roundtable in terms of how they would have to deal with maybe as many as 30 or 40 different standards, as I would figure that a number of States might join up with and team up with others? What is the reaction to that? It goes along with what Ms.—

Ms. ZHENG. Yes, we strongly believe that a fragmented sort of regulatory environment where we pursue a State-by-State sort of regulatory approach to privacy makes for very inconsistent consumer protections. It also creates massive barriers to investment and innovation for companies that have to operate in all of these different States. It is simply unworkable.

And so that is why we think it is necessary to have a single national Federal privacy law that preempts State laws. And I think the assumption that preemption weakens existing privacy protections is a false assumption. You know, we strongly believe that a Federal consumer privacy law should be strong and should provide additional protections for consumers that are consistent across every State in the country.

As I think, you know, folks here mentioned earlier, devices, data, people, they constantly move across borders, across States. A State-by-State approach just simply doesn't work for this type of domain. And, in fact, even when you look at California's own privacy law, there is a rather strong preemption clause in the California law that preempts city, county, and municipality laws within the State of California, likely for exact same reason why a Federal privacy law should preempt State laws.

Mr. UPTON. And are you aware, is anyone tracking what the other 49 States might be doing?

Ms. ZHENG. We are. I think a lot of folks on this panel are as well.

Mr. UPTON. Yes. And are any of those States getting close to something like California has done? I know it is a new legislative year for many States, but—

Ms. ZHENG. There are a number of—

Mr. UPTON [continuing]. What are your thoughts on where other States may be?

Ms. ZHENG. Yes. I think there are roughly about 30 different State legislative proposals related to privacy. They all take, many of them take very, very different approaches or regulate certain types of sectors. Some of them are more general. Some of them may be focused on specific types of information that are personal. But

what it demonstrates is that there is a ton of interest within the States and they are not taking a coherent, consistent approach.

Mr. UPTON. And what are your thought—do you think that any of these States will actually do anything yet this calendar year or not? I know that it is early.

Ms. ZHENG. It is hard to say, but I think it is highly, highly likely that a number of States will pass privacy laws this year.

Mr. UPTON. I know I don't have a lot of time left as I ask my last question, but I thought that Mr. Grimaldi had some very good comments in his testimony about four different parts to achieve the goals. One, to have clear prohibitions on a range of harmful, unreasonable data collection; two, is that the new laws should distinguish between data practices that pose a threat to consumers and those that don't; three, that the law should incentivize a strong and enforceable compliance and self-regulatory programs; and, finally, that it should reduce consumer and business confusion by preempting the growing patchwork of State privacy laws.

As it relates to the first three, knowing where I think I know you all are in part four, where are you in terms of your thoughts as to those first three principles? And maybe if we can just go down the line and we will start it with Ms. Collins-Dexter as to whether she thinks that is a good idea or not, briefly, knowing that I have a minute left.

Ms. COLLINS-DEXTER. Could you repeat that one more time? Apologies. I was like taking furious notes.

Mr. UPTON. So Mr. Grimaldi had three, four points of which I think that the first three that I would like to focus on. One, that the clear, have clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified by the law, these are goals for legislation. Two, that the new laws should distinguish between data practices that pose a threat to consumers and those that don't. And third, that the law should incentivize a strong and enforceable compliance in self-regulatory programs.

So I guess now we just have to go to yes or no with 20 seconds left.

Ms. COLLINS-DEXTER. Yes.

Mr. UPTON. Dr. Layton?

Dr. LAYTON. Yes.

Mr. UPTON. Ms. Zheng?

Ms. ZHENG. Yes.

Mr. UPTON. And Ms. O'Connor?

Ms. O'CONNOR. Yes.

Mr. UPTON. OK.

Ms. O'CONNOR. The self-regulation alone is not going to be enough. That was revolutionary in 1999, but it is no longer sufficient to protect consumers today.

Mr. UPTON. My time has expired. Thank you.

Ms. SCHAKOWSKY. I now recognize Mr. Veasey for 5 minutes.

Mr. VEASEY. Thank you, Madam Chair. You know, earlier, in Ms. Collins-Dexter's testimony something really, you know, concerned me and really hit home for me when she was talking about, you know, how poor people are being targeted for some of this marketing and these privacy issues that we are having. And for a lot

of the people that do fall within that category, it is going to be very important for them that these services remain, quote unquote, free, whatever free is. And of course we know that nothing is really free.

And what is so troubling about that is that in our society obviously we live in an economy that is based on profit and gain. What is the sweet spot? I would like to know maybe from Ms. Zheng or Mr. Grimaldi from a business standpoint what is the sweet spot? How can you still provide these services for free for the constituents that I represent and the people that Ms. Collins-Dexter was talking about, how do you preserve them being able to access this without them having to pay additional fees, but the market research and the other things that go along with these services being free, and how do you combine all of that? Is there a real sweet spot in all of this?

Ms. ZHENG. So I think—thank you for that question, Congressman. It is a really important issue and I am glad that you raised it and I am glad that Ms. Collins-Dexter raised it. It is complex. It requires additional attention. There is significant technical, legal, and ethical considerations as well. Companies should not be using personal data about consumers to make discriminatory decisions in the areas of employment, housing, lending, insurance, or the provision of services.

But defining that line between using an algorithm to discriminate against consumers and using it to target, for example, ads in Spanish to Spanish-speaking consumers is challenging. So we need to be mindful of some of the more, these legitimate uses of certain demographic information that enable products and services to be better tailored to a consumer.

But we recognize that this is a really important issue as is the, you know, differential pricing issue that you raised. Although we have significant concerns with the particular approach taken in the California law, we welcome the opportunity to work with the committee on this issue and consider different proposals though. Thank you.

Mr. VEASEY. For the areas where these companies are trying to obviously maximize their return on investment where they need control groups and run tests, can that still happen, Mr. Grimaldi, with more consumer protection? And obviously the consumer protection is definitely needed. I think that you can just listen to just a very few minutes of today's testimony and realize that.

Mr. GRIMALDI. Correct, Congressman Veasey. Associating myself with Denise's comments, we need to break apart any discriminatory practices from good practices. And you mentioned the value exchange that goes on behind consumers transacting their business on the internet and Chairman Schakowsky went through a long list of what she has only done in the last 48 hours going to a store, taking a flight, et cetera. Those are useful practices that people come to accept. However, that information cannot be gamed for reasons of eligibility, of discrimination, of price discrimination. Our industry is absolutely against that.

There is a self-regulatory code that our companies adhere to in the Digital Advertising Alliance, a body that we stood up, stipulating to what Ms. O'Connor has said in that self-regulation, the reason that we are here, we need help apart from self-regulation.

We are here to partner with Congress to say it is past time, we are overdue in a national framework that speaks to these issues.

But yes, there are good uses. There are harmful uses. That is what we need to break apart and distinguish.

Mr. VEASEY. Madam Chair, I yield back. Thank you.

Ms. SCHAKOWSKY. I now recognize the ranking member of the full committee, Mr. Walden.

Mr. WALDEN. Thank you, Madam Chair. And as you know we have another hearing going on upstairs, so I'm having to bounce back and forth.

In the United States we currently enjoy an environment that allows small to medium-sized companies to grow, to raise money and compete and in large part because they do not have to come to the government to get their business plans approved and how we have successfully legislated based on well-defined risks and harms.

Dr. LAYTON, if data sharing and privacy is regulated differently by individual States in the U.S., what will that do to the American marketplace?

Dr. LAYTON. So assuming this could pass a court challenge, because I think it would violate the commerce clause as we discussed, I don't see how it is possible you can send products into other States if you are a retailer in Maine and you have to send your products to 50 different States and you have to have 50 different ways to do it. I don't see why you would start that business. I think you would move to another industry.

Mr. WALDEN. So how has GDPR impacted Google's market share in the EU?

Dr. LAYTON. It has increased since it came into effect.

Mr. WALDEN. And I think that is what we are showing right here on the slide that nobody could read from afar, I am sure. Maybe we can put it on the big screen and take me off, which would be a pleasant experience for everybody. But I don't have a copy of that here at my desk.

[Slide.]

Mr. WALDEN. But I think what you are seeing here is that small innovators are actually leaving this space, right? And investment in small entrepreneurs is going down in Europe and going up in the United States since GDPR was put in place. Is that accurate?

Dr. LAYTON. Yes. So this particular graph is looking at what is, what they are highlighting here is the competitor, the analytics competitor. So Google Analytics is running on a lot of websites and depending on the company they may have multiple competitors to Google Analytics. Retailers have a set, you know, different sorts of areas.

So essentially some media companies, some larger firms are kicking off the smaller competitors for their—they are kicking them off, so that means that those trackers have not been firing. That is what this is measuring.

Mr. WALDEN. Yes. My understanding shows that shortly after GDPR was implemented, Google's market share increased by almost a full percent and smaller ad tech firms suffered losses of anywhere from 18 percent to almost 32 percent. GDPR has proven to be anticompetitive and makes it more difficult for small businesses to compete and just one example of that negative impact.

Now there may be other things going on affecting these numbers, I will stipulate to that. But clearly GDPR has had an effect.

Mr. GRIMALDI, since GDPR has been in effect, academic research shows that investments in startup companies in the EU have dropped by an aggregate of 40 percent, 4–0. Compare that to the United States, where in 2018 investments and startups neared \$100 billion, which is the highest year since the dot-com boom, protecting consumers including protecting them from a marketplace devoid of choices so they are forced to use certain products or services.

What should an American approach to data privacy look like and that does not hamper small business and investment?

Mr. GRIMALDI. Thank you, Chairman. You are correct. We are seeing that fall off in Europe and it is not because—I listed some newspapers at the beginning that are not currently operating in Europe and it is not because they are not complying with the law and it is not because they were at fault. It is because they just can't afford that kind of a pivot to construct their services that could be at legal risk, at great legal risk.

This is one of the many things that we are seeing with CCPA that is going to be a major deterrent, if not a killing blow, to American companies that can't deal with the labyrinth in construct of new regulations in California, or other States that might force them to take down their online advertising funding regime for fear that they could be susceptible to a major lawsuit because they did not classify or categorize data in a way that could be returned to consumers.

Because they currently, these companies don't have those structures in place and now in order to do something that again I stipulate was correct in its founding—transparency, choice, accountability—is now potentially going to force companies to say we just can't afford to retrofit all of our systems and be able to collect that much data, and even if we do there is a litigation risk that we wouldn't be able to swallow. So.

Mr. WALDEN. Could you put that litigation risk in common person's terms? What are we talking about here if you are a small business online?

Mr. GRIMALDI. Correct. Under CCPA some of the provisions—and we are active as I think many in this room are in dealing with the California Attorney General's Office, former Congressman Xavier Becerra being that Attorney General. He is taking a look at the current law and promulgating it to be enforced in January. The litigation risk could mean that if a consumer requests their data from a company, if a consumer reaches out and says, "What do you have on me and how is it shared," a company has to be able to provide that in a certain time frame. And if it doesn't, it is in violation of the law. That litigation risk you can compound into the thousands or hundreds of thousands of requests that will multiply into the millions and billions of dollars. And that is something that smaller companies would not be able to deal with.

Mr. WALDEN. My time has expired. I thank all of our witnesses for enlightening us in this issue. Thank you.

Ms. SCHAKOWSKY. And now I yield to the chairman of the full committee, Mr. Pallone.

Mr. PALLONE. Thank you, Madam Chair. I wanted to build on your questions. Some uses of our data is certainly concerning. This committee has explored many of them, Cambridge Analytica's use of people's data to manipulate their political opinions and influence their votes, for example. And we had hearings with Equifax, Facebook, and Twitter.

We can't begin to reveal just how little we all know about who is collecting our data or what they are actually collecting. And I think many of us have this vague idea that everyone is collecting everything and that there is nothing we can do about it, but in my opinion that is not acceptable because some data maybe just shouldn't be collected at all.

So in that vein I wanted to ask Ms. O'Connor, data collection has become extremely profitable leading some companies to collect every bit of data they can, but is there a line that shouldn't be crossed? Should there be some limits on actual collection?

Ms. O'CONNOR. It would be our position that yes, at least as to the most sensitive information there should be very clear notices and awareness on the part of the consumer, again the example I used of my fingerprint in my phone being collected for one purpose, not being used for any other. When I use a map app they obviously need to know my location. I do not want that location sold or transferred.

Are there types of data that shouldn't be collected at all? In our bill, in our proposal we look very seriously at issues of precise geolocation, biometric information, children's data, content of communications, and health information as deserving higher sensitivity and higher protections.

Mr. PALLONE. All right. Let me ask Ms. Collins-Dexter, how do you think we should be—well, how should we be thinking about limits on collection and what about limits on sharing, sharing with or selling to third parties?

Ms. COLLINS-DEXTER. I echo Ms. O'Connor. I think we should be looking at all of this right now. Companies have a financial incentive to collect as much information as they can and store it forever with no obligation not to do that. I think we have to have meaningful data minimization requirements. I think we have to definitely look at the various ways in which information is often used as a proxy for race.

So, for example, we know that Facebook and a lot of big tech companies actually don't collect explicitly race data. However, many things around geolocation and daily habits are able to like put together this data profile in which like people are able to ascertain race and that is used for predatory marketing practices.

And so we have to be able to like parse through all of that information and keep a constant eye on impact, which I think should be at the core of any legislation that we are looking at.

Mr. PALLONE. Thank you.

Ms. O'Connor, what about limits on sharing with or selling to third parties?

Ms. O'CONNOR. Absolutely. We put those in two separate buckets. First, limits on sharing again for the most highly sensitive of the categories I mentioned, particularly things that are immutable or most intimate about you. On selling we would also put limita-

tions, or sharing with third parties that the third parties would have to be bound by whatever promises the first party made about that data.

So absolutely, we would look very hard and limit secondary use and third-party sharing.

Mr. PALLONE. Thank you. I just wanted to ask about limits on sharing people's information with affiliates, because we know that many corporations own multiple affiliated companies that the average person would not contact, like YouTube, Android, and DoubleClick are all owned by Google, or Jet.com and Sam's Club both owned by Walmart. Data collectors who say they don't sell data to third parties may still want to share that with their affiliates.

So let me ask Ms. Collins-Dexter, should there be limits on sharing people's information with these corporate's affiliates?

Ms. COLLINS-DEXTER. Yes, absolutely. We should definitely be looking at how these third party companies are operating as we saw with Facebook last week and as we continue to see with, as you all have mentioned, Cambridge Analytica and others. You have these third-party data mining companies that aren't regulated, aren't looked at. They are gathering data, scraping it, selling it to companies for predatory marketing purposes, selling them to like law enforcement without our consent and because we don't even know that these companies are looming in the background it really even further limits our choice or ability to say no.

Mr. PALLONE. And just quickly, Mr. Grimaldi, behavioral ads, advertising needs data to target as to the most appropriate audiences. How would limitations on the collection and retention affect your member companies? Are there limits that can be established through legislation that provide reasonable protections to consumers that your member companies would accept?

Mr. GRIMALDI. Sure, thank you. We currently have a very robust, self-regulatory program that is targeted to consumers having transparency into their online behavioral advertising and the ability to click through the ad via an icon in the upper right corner of every ad that is served over a trillion times per month that takes you to a page that says, why am I seeing this ad and how can I stop seeing it?

There is tremendous uptake in terms of people going through that ad up to the tune of about 70 to 80 million unique impressions. So we offer that control. One of the messages today before you is as much as we are trying to educate consumers on that there is still a need for a Federal program that can help us distinguish what kind of advertising is working, what is considered harmful and what do consumers need to know.

Again before they click on something it could be something that is very much tailored to what they are looking for, an ad that speaks to them. We have much research that shows that consumers prefer targeted behavioral advertising rather than generic advertising, but we want to make sure consumers have those controls so that they can stop seeing those ads and again that could be enshrined.

Mr. PALLONE. Thank you.

Ms. SCHAKOWSKY. And now I yield to Mr. Latta, the former chair of this subcommittee and my friend.

Mr. LATTA. Well, thank you very much. If I could ask just a quick point of personal privilege and congratulate the Chair on assuming the gavel. So congratulations, it is a great subcommittee.

And Madam Chair, before I begin I would also like unanimous consent to enter into the record excerpts from the WHOIS report from the Department of Justice Attorney General's cybersecurity task force.

Ms. SCHAKOWSKY. Sorry. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. LATTA. Thank you, Madam Chair, if I could reclaim about 30 seconds there.

Last Congress, the Energy and Commerce Committee held nearly a dozen hearings discussing privacy and security issues. That includes much publicized hearings where we heard from the CEOs of Facebook and Twitter about how the companies collect, safeguard, and use data. From those hearings it was clear that while these companies provide a service that Americans like, consumers aren't always clear about what happens with their personal information.

With the California law slated to take effect at the beginning of next year, time is of the essence. In divided government it is not always easy to tackle the tough problems, but I believe the time is right to work together on a Federal data privacy solution. Both consumer groups and business organizations have come onboard in calling for a national standard. We all agree that consumers should have transparency and accountability and that we want to ensure that the United States stays the prime location for innovation and technology.

Dr. Layton, if I could ask you, I have been hearing from many groups regarding the loss of access to information about domain name registration or the WHOIS data and the role it plays in protecting consumers. Would you explain how WHOIS increases online transparency so that consumers may have a better understanding of who they are interacting with online?

Dr. LAYTON. Right. So the WHOIS database, for just lack of a better way, would be a sort of address book for the internet, who is registered, who owns what particular domain.

Mr. LATTA. And following up, would you want to comment on how the GDPR is creating challenges to accessing that data?

Dr. LAYTON. Absolutely, so one of the key problems is that because of its ability to retract information, that people are—that the domain name registers are masking their identity. This is making it very difficult for law enforcement to find out perpetrators of crimes. It is also an issue to if you need to contact things where intellectual property, for example.

So there are many concerns with this and this reflects, you know, our historical view of privacy of prioritizing the right to know. We believe that the public has a right to know about these things.

Mr. LATTA. Well, could you go into a little more depth about on how, you know, that information helps in identifying those bad actors and those criminals that are out there and that law enforcement needs to be able to find those individuals and bad actors?

Dr. LAYTON. Right. Well, in just the same way that if you looked at a phone book and you would see, well, you know, a certain address and this place, who lives at that address, I mean that is a key function of law enforcement. So if you are taking that away for the internet for global, for law enforcement everywhere that it is a serious problem.

Mr. LATTA. And if you could list your top three concerns for the GDPR and also the CCPA which is the California law?

Dr. LAYTON. Sure. Well, I would say the first concern from the U.S. perspective would be First Amendment free speech concerns that the level of government requirements is so high that it reduces expression. That would be number one. I would certainly say safety would be number two with regard to just what you described. You have other issues with people who have committed crimes in the European Union who are asking that their records be erased or removed that have committed murders, child molestation, and so on. That is a serious problem.

And I would say thirdly, the sort of a dumbing down of consumers that there is creating a false sense of security that somehow that regulators have the answer on what to do, it doesn't allow consumers to take responsibility for when they go online. And I would add number four, which is I think that you are freezing in place technologies and you don't let them evolve.

So, for example, the EU will require using certain kinds of data protection technologies, but we can actually make them better. So if you require a company to do technology A today, I can invent technology B tomorrow and I am not allowed to upgrade to it. So that is a major problem as well.

Mr. LATTA. All right, I appreciate it very much and I yield back the balance of my time.

Mr. O'HALLERAN [presiding]. Next will be Mr. Luján, New Mexico.

Mr. LUJÁN. Thank you very much, Mr. Chairman, for this important hearing. Let me jump into this.

In 2000, the FTC recommended that Congress enact a consumer internet privacy legislation. That was 19 years ago. This subcommittee held a hearing after the Equifax breach in 2017. We had Mark Zuckerberg before the full committee in April 2018. The 115th and previous Congresses failed to pass meaningful privacy protections even though there were commitments made to the American people.

So as we jump into this, Ms. O'Connor, an entire economy based on data has been built but we didn't stop to consider the risks and potential downsides companies collecting data have put consumers at risk.

Mr. Grimaldi, in your testimony you say that the law should incentivize strong and enforceable compliance and self-regulatory programs by creating a safe harbor process, but I am concerned that incentives won't be enough. We need some accountability. So what one of the ideas that we have is to require companies to conduct risk assessments, if you want to process data for consumer-related uses you need to assess the foreseeable risks of such uses.

So, Ms. O'Connor, yes or no, should we require risk assessments so companies factor the risk and potential harms in their decision making?

Ms. O'CONNOR. Certainly the concept of risk assessments or privacy impact assessments has been around since even before those FTC hearings, which I attended in the year 2000 and before, and certainly that is part of a robust privacy program. But we do want to be mindful of the burden on small businesses and make sure that the legislation that is comprehensive is elegant and efficient. It is simple. It is streamlined and easy for a small, a medium, and a large company to know what the rules are and to abide by them.

So while I am certainly in favor of and I have implemented a number of PIAs or risk assessments in my time in the government and in the private sector, I want to make sure that the law is simple and clear for consumers and for companies.

Mr. LUJÁN. So assuming the same disclaimer holds true to the next question, yes or no, should we require a privacy protection officer at companies that collect large amounts of data who would be responsible for training staff, conducting audits, working with authorities, and advocating for privacy with the entity?

Ms. O'CONNOR. Yes.

Mr. LUJÁN. There is a great editorial that was authored in Forbes, January 15th, 2019, titled "2019 Data Privacy Wish List: Moving From Compliance To Concern." I would ask unanimous consent to submit it into the record.

Ms. SCHAKOWSKY [presiding]. Without objection.

[The information appears at the conclusion of the hearing.]

Mr. LUJÁN. In it one of the points that was made here is from a move from privacy compliance to concern and care. That "rather a philosophy that treats data with extreme care and with prevention of data breaches in mind," that that is something that companies should be doing. So that is where I am thoughtful from a incentive perspective, but what we must be doing going forward.

Ms. COLLINS-DEXTER, you highlighted in your testimony some important aspects here. And I am concerned about implications for access to housing, lending, digital redlining, and voter suppression as we talked about information that is shared that is sensitive. Would you agree that this is a problem?

Ms. COLLINS-DEXTER. Yes. I absolutely do.

Mr. LUJÁN. Have companies responded when it has been brought to their attention that their products or services are having discriminatory effects?

Ms. COLLINS-DEXTER. On the whole, no, it has not. We have sat at the table. Part of our model is a corporate accountability model which requires direct engagement in negotiation. We have sat at many companies, Facebook included, for many years and have a lot of discussions with them. And for every policy they develop we tend to find weeks, days, months later that the problem is really much larger than what was initially indicated. And so self-regulation has not proven to be a viable option.

Mr. LUJÁN. So with that being said, have the responses from industry been adequate in this space?

Ms. COLLINS-DEXTER. Have the responses from the industry?

Mr. LUJÁN. Been adequate?

Ms. COLLINS-DEXTER. No.

Mr. LUJÁN. Are there changes companies have made voluntarily that should be made into law? And we can get into the details, just yes or no.

Ms. COLLINS-DEXTER. Yes.

Mr. LUJÁN. So we would be happy to work with you in that space.

Mr. Grimaldi, the IAB represents over 650 media and technology companies that together account for 86 percent of online advertising in the U.S. You heard the quote that I referenced from this editorial. Are these companies looking to protect my privacy when they are making business decisions?

Mr. GRIMALDI. Congressman, they are. They are without a doubt. One of the things again why we are here today is to ask government to fill in those holes that we can't fill in. Should there be mandatory components of a privacy policy that does not let a user accidentally click something to give consent? Is there other pieces where we could work with you on strengthening what we already have put in the market for consumer controls.

Mr. LUJÁN. Let me ask a question as my time expires and I will be happy to submit that to the record so we can get a response. Would you agree that companies need to shift to a philosophy that treats data with extreme care with prevention of data breaches in mind?

Mr. GRIMALDI. I think what needs to be defined are those unreasonable and reasonable uses of data. Again many on the committee have said we use data, we give our data to certain apps or to certain programs to help us every day. Is that data being used for those purposes? Are there harmful uses of data? I think the absolute answer is yes. Are there guardrails we can put around it, more self-regulation, more partnership, yes.

Mr. LUJÁN. Madam Chair, just as my time has expired and I thank you for the latitude here, it just seems that we wouldn't be here today if, in fact, there was an effort to concern and care versus just compliance. And I think that is what we are looking for is how can we work on this collectively and together such that we get to that point. So I appreciate that time. Thank you, Madam Chair.

Ms. SCHAKOWSKY. I recognize for 5 minutes Congressman Bucshon.

Mr. BUCSHON. Thank you, Madam Chairwoman.

I was a healthcare provider before, and health information is some of the most sensitive information that is out there and it is also some of the most valuable. So I hope that whatever we do here in Congress specifically addresses health information because it is really critical and important.

As you may have heard, last week it was revealed that Google's Nest Guard home security device had a microphone inside the device that consumers did not know about and it was not disclosed. As I have discussed in prior hearings on data privacy including with Mr. Zuckerberg, I am concerned about the inappropriate collection of audio data. And it seems that everyone denies that that happens, but I think everyone knows that it probably does.

So Ms. Zheng, can you expand on how the right to privacy would play into this type of practice and how we would deal with that?

Ms. ZHENG. Thank you for that question, Congressman. When it comes to audio data if it is personally identifiable information or personal information and falls within the scope of a privacy, you know, a new privacy bill, I certainly believe that transparency, control, access, the right to correct it, the right to delete it, should be rights the consumer should have including for audio data.

Mr. BUCSHON. Because that is going to be important because if we exclude things that you actually type on the internet but we don't have things in privacy where if you are talking your phone picks it up and sends a keyword to someone and they advertise based on that, then we are missing the boat on that. I want to prevent collection of data without consumers' knowledge and audio data would be there.

And, Dr. Layton, do current laws cover this type of omission from Google about a microphone? And second, if we decide to grant additional authority to the FTC, would you have any suggestions on how the FTC may play a role on addressing intrusive data collection policies including audio data without harming innovation?

Dr. LAYTON. Thank you, Congressman. I think it is excellent that you raised the point when you use various devices in your home, Alexa home and so on, you are having conversations with your family members. And I think law enforcement has actually used some of that data in some cases and with good purposes for it, actually. In terms of the Federal Trade Commission, they are engaged in this process now. I don't know if audio is a specific part of their inquiry. I would have to get back to you on that.

Mr. BUCSHON. OK.

Dr. LAYTON. I can't recall at this moment. But I don't see from a technical perspective why audio would be different because it would be recorded as the same data. Even though you are speaking it, it would be transcribed into a data file, so.

Mr. BUCSHON. OK. The other thing I want to quickly say, and then I have a question for Mr. Grimaldi, is that also we need to address hardware as part of this. Not just an app but hardware, because data, location data is really important. And there was a local news media here in town who turned off their phone and did everything they could except take the battery out. Went all over the city of DC and then went back, plugged it in, and all the metadata everywhere they were was recorded, and as soon as they turned that phone on it all went out to the internet. So hopefully anything we do on privacy also includes hardware, not just apps, not just software. That would be important.

So, Mr. Grimaldi, in your testimony you highlight that data-driven advertising has helped power the growth of the internet by delivering innovative tools and services to consumers. Many constituents including myself, and I am going along the audio theme here, have concerns about how conversations when not directly using an app, device, or other electronic device appear in a later online ad based on keywords in the conversation. Can you help me understand how this is happening?

Mr. GRIMALDI. Sure. There is—and also I think it is important to understand the difference between personal data and synonymized data. And that is if you were using, if you were in your conversation using words that were flagged that weren't, you know,

Congressman Bucshon, but they were an individual who was into hunting or was into automotive, cars, you name it, sports, that data could be tagged for you and used to serve you better targeted ads.

Mr. BUCSHON. Can I just interrupt for a second? So I was having a conversation with my communications director, this happened about a month ago, talking about a certain subject and the next day he got ads on his computer specifically about that particular subject. We happened to be talking about tennis because he is a tennis instructor, but nonetheless. So continue.

Mr. GRIMALDI. Right. And without intimate knowledge of how that hardware is constructed, if I were to take that as an example of just your web browsing those sorts of things could be flagged in order to serve you ads that are not generic, that are more tailored to your interests and done in a way that again the word “synonymized,” meaning you are put into a category rather than your name, your address, your Social Security Number, but just your likes and dislikes. And then that enters a marketplace behind the web where that information is used to serve you better ads without linking you personally to your information, your intimate information. It is another piece of that reasonable and unreasonable construct we are talking about.

Mr. BUCSHON. OK. My time has expired, but I want to make sure that whatever we do here in this committee it includes audio data and also considers location data based on hardware within a device. Thank you very much. I yield back.

Ms. SCHAKOWSKY. I recognize Congresswoman Rochester.

Ms. BLUNT ROCHESTER. Thank you, Madam Chairwoman. And thank you so much for setting the tone of this hearing and this is a vitally important topic for Delawareans but also for our Nation, and I want to thank the panel as well.

You know, more and more in our daily activities they involve the use of the internet. Many of us pay our bills, shop, play games, and keep in contact with friends and relatives through websites or online applications. However, with all of these activities taking place online, websites are amassing more and more personal information. This presents serious privacy concerns.

Large-scale data breaches are becoming more common and consumers have a right to know what is being collected, how it is being used, and should be notified when a breach has occurred. Most of you on the panel today have discussed the need to give consumers more control over their own information, to get more control over their own information and should it be, you know, how it should be collected and how it should be used.

And I want to drill down just a little bit deeper on that and ask Ms. Zheng, the Business Roundtable’s privacy framework promotes the idea of giving the right to access the correct, and correct inaccuracies in the information collected about them. So can you talk a little bit about what you mean by information collected about them and does that just refer to data points collected or does it also include any inferences made based on that data?

Ms. ZHENG. Congressman, that is a good question and it is a very specific and detailed question that to be honest with you we still need to discuss within our membership. Right now as we drafted

our proposal, our framework, the right to access, correct, and delete your data does apply to your actual personal data. So, but to answer your further question I would need to follow up with you.

Ms. BLUNT ROCHESTER. And I am going to ask a few other people questions around this as well. I mean I think a lot of us are familiar with, you know, the story of the individual at Target who got the coupons, came to the father's house for a pregnant teen, and again it was inferences.

And so I want to ask Ms. Collins-Dexter, what are your thoughts on access and correction and should consumers be able to see and correct inaccurate inferences made about them? And I want to start with you.

Ms. COLLINS-DEXTER. Yes, absolutely. We think that people should, similar to a credit report, have an opportunity to challenge and correct information. One of the things that we have even seen with some of our work around voting records and purges that have happened across the country is that there is a lot of data collected and based on like inaccurate names or misspelled names that allow for voters to be purged from files across the country.

I think, you know, as we think about all of the various data points and all of the mistakes that happen, again we are finding the people that tend to be most impacted are low-income communities of people of color, people who aren't able to actively challenge and correct the record on themselves. So I would say it is extremely important on a number of different fronts that we are allowed to do that and any privacy legislation should allow for that.

Ms. BLUNT ROCHESTER. Thank you.

And, Mr. Grimaldi, you didn't really talk about consumers' right to access and correct information collected in your testimony, but how do you think giving those rights to consumers would affect your member companies?

Mr. GRIMALDI. Thanks, Congresswoman. To echo what some of my co-panelists have said, consumers have a right to delete their data and I think there are things to explore with those rights. There are obviously fraud, misuse, other components that could negatively affect either a consumer's online experience or their just life experience, and we are seeing that contemplated in Europe and we are seeing that contemplated in California. There are problems though I would point out that could come about when consumers request their data to be deleted and the authentication of those consumers requesting it.

One of the major pitfalls that we are currently working on with the California law is if somebody could have their data deleted, how do they authenticate themselves to make sure it is them? If somebody can request their data, how do we know it is them and it is not somebody stalking them or somebody meaning to do them harm. Those are really important questions.

Ms. BLUNT ROCHESTER. You know, I want to kind of close out my comment by just saying that why this is so important is because I think a lot of people do feel that it is a fait accompli. This is the world that we now live in. And that is really what the role of Congress is, is to make sure consumer protection going back to what our chairwoman said. Thank you so much. My time has expired.

Ms. SCHAKOWSKY. I now recognize for 5 minutes Congressman Carter.

Mr. CARTER. Thank you very much, Madam Chair, and thank you, all of you for being here. This is an extremely important subject and we want to do the right thing, so that is why we got you here. You are the experts. You are the ones we want to learn from and hopefully build upon.

Dr. Layton, I want to start with you. First of all, earlier, one of my colleagues mentioned the WHOIS database. Can you explain that very briefly what that is exactly?

Dr. LAYTON. Well, I just use the address book for the internet, you know, those who registering the names that they have to disclose who they are.

Mr. CARTER. Well, it is clear through your testimony as well as your background that you have a good grasp of GDPR and the impact that this had. It is my understanding that the WHOIS, or ICANN is the governing agency over WHOIS, that they have actually run into problems with this and they have actually said that they are not going to be collecting that data anymore?

Dr. LAYTON. So, no. They have actually for some, for quite a long, at least a year they have been trying to work with the officials in the European Union to highlight to them the problems and to find a resolution. And the pressure from the, you know, extreme privacy advocates in the European Union are not letting them come to a resolution. So as I understand today, I don't have the most up-to-date, but I think there is an impasse right now because it is not resolved. So the information is not available.

Mr. CARTER. Well, this is the kind of thing that we want to learn from. I mean we don't want to make the same kind of mistake that obviously they have made and because it is my understanding that WHOIS data is very important particularly to law enforcement. Has that been your experience?

Dr. LAYTON. Yes. Well, absolutely. I mean it is a major issue for law enforcement, intellectual property rights holder, you know, people in the public who may need to do research and so on. I think the lesson learned here is, you know, we have heard before the way to hell is paved with good intentions. I think everyone has had good intentions and they have overreached. They went too far. They didn't have a process to test the various provisions. Everybody got to tack on what they thought made sense and then they just bring it over the finish line and we have to live with it.

Mr. CARTER. What do you think we could learn from that? I mean how could we make it better?

Dr. LAYTON. Well, at least one of the things I would say in terms of how we are ahead in this respect, in the United States we have a transparent policy process. When we are submitting anything to the Federal Trade Commission, as part of what they are doing you have to disclose your name, who you are, you are conducting this hearing today.

The policy process now in the EU because of this rule means you can mask your identity. So you can submit into a regulatory hearing, you don't have to say your name. You don't have to say who you are, for privacy reasons. So what I would encourage Congress to do is keep with our tradition for the public's right to know, to

continue in this vein as you are having the hearings today, and to, you know, to take these steps to look at where it hasn't worked and to not make the same mistakes.

Mr. CARTER. Let me move on. Earlier we talked about market share particularly as some of the companies have grown in market share and at the expense of others as a result of the GDPR. What is the primary reason for the change in market share for some of these companies?

Dr. LAYTON. So, well, in many respects there are, it is because a number of firms have exited the market. They have decided they are no longer going to operate, so in many respects that the advertising market has shrunk in the sense that there are fewer properties on which to conduct advertising that would be one thing. The other issue is that when those other smaller players leave it just means that people visit the larger players more.

Mr. CARTER. Has this had an impact, obviously it has had an impact on the exports to Europe of various content and digital goods?

Dr. LAYTON. Right. Well, so for me when I am sitting in my office in Copenhagen and I try to go to Chicago Tribune, I cannot open it. I just see a white page that says, "Sorry, we are not delivering our content." And, you know, that is unfortunate for me, I can't see the information. It is too bad for the advertiser, they can't put the advertisement on the page. It is sad for the 1 million Americans that live in the EU.

Mr. CARTER. I was about to say it obviously has an impact on them, and they are not able to get the information.

Dr. LAYTON. Right. So, but I think as Mr. Grimaldi, he pointed it out very well and I think his testimony makes it very clear it is not that they don't want to do it, but it costs too much money and there is a regulatory uncertainty. The legal risk is so high because it is not just—it is so new, this rule, so we don't know how they will be interpreted and it is a whole value chain that all of the partners who might be working with Chicago Tribune or whom-ever may also be liable. So they don't want to take the risk.

Mr. CARTER. Well, again I want to thank all of you for being here. I think there are important lessons that we can learn from the experiences about the European Union as well as what we are trying to do in California. Obviously what we don't need is 50 different sets of rules governing. We need one set of rules here in America.

And hopefully, and I have always said I don't want to stifle innovation so that is one thing I hope we keep in mind in this committee as we move forward. Thank you, Madam Chair, and I yield back.

Ms. SCHAKOWSKY. Thank you. And now I welcome the vice chair of this committee, Mr. Cárdenas.

Mr. CÁRDENAS. Thank you very much, Madam Chair, and thank you for holding this very important matter before the public. And to the ranking member as well, thank you.

Ms. O'Connor, would you like to shed maybe a little bit of light on the dialogue that we just witnessed over the last 3 or 4 minutes about the EU and maybe the mistakes they made and things that we could learn and the cross reference between innovation and privacy?

Ms. O'CONNOR. Thank you so much, sir. I think it is fairly certain that we in the United States will pass a United States law that reflects our values and our cultural traditions and our unique opportunity here as the birthplace of Silicon Valley. But I think there are also our shared values, values of respect and dignity, values of customer trust that our companies, our U.S.-bred companies can certainly adhere to.

I think privacy and security are a form of corporate social responsibility in the digital age and are essential to doing business in a thriving U.S. economy and around the world. Yes, it is important to get to a Federal standard, but it is important that that standard be strong and be understandable by small, medium, and large enterprises in the United States and, most importantly, be one that customers can trust, that consumers and citizens of this country can have certainty that their information is being treated fairly, that they are not being discriminated against, and that they understand the consequences of the bargains that they strike with companies.

Mr. CÁRDENAS. Well, one thing that I enjoy the most is being able to go back to my district and I am blessed that my two grandchildren live in my district, so I can drive 5 minutes, jump on the carpet and roll around with them and play with them and know that when they grab a toy—like my 6-month-old, she is at that age where everything goes in her mouth—know that consumer protection is something that we take for granted in this country. We didn't do that back in the day maybe decades ago, but at least today I know that there is a 99.999 percent chance that that toy is not going to hurt my little granddaughter.

Speaking of children, under the CCPA businesses are supposed to provide an opt-in mechanism for children 16 and under to allow companies to sell their personal information as defined by the CCPA. How do they know whether the children are 16 and under, under any system?

Ms. O'CONNOR. Well, that is such a great point because it requires more authentication and more knowledge in order to know who your consumer is. I think you have identified one of the very compelling gaps in our coverage right now, the above COPPA but below majority age group in our country. I have several of those people living in my house right now and they are a challenging age on the internet to say the least. And it certainly bears consideration of what we should do going forward to consider whether COPPA is working adequately and what to do with that in-between age group.

Mr. CÁRDENAS. What is the mechanism to get parental consent for children under 13?

Ms. O'CONNOR. It is somewhat complicated and requires several steps of the parent self-authenticating and providing phone numbers or email addresses or the like. I seem to do this every single day on my computer for my youngest child. But it still is fraught with some peril that the child may be providing inaccurate information or that the data may be used in a way that is unanticipated by the parent or the child.

Mr. CÁRDENAS. Under the Federal law COPPA companies must obtain parental consent before collecting personal information on-

line from children under the age of 13. How do companies verify parental consent and how does the FTC enforce this?

Ms. O'CONNOR. The parent often has to respond to an email verifying that they are the parent or that they have authorization. The FTC has taken some cases and I think there is concern in the marketplace about whether the enforcement mechanisms have really fully grasped the complexity of the issue both in the online world and as you point out in the Internet of Things world.

Mr. CÁRDENAS. What seems to be the logic or the history on the difference between a 12-year-old and a 13-year-old, and why is that the cutoff point?

Ms. O'CONNOR. I am sorry. I can't speak to the legislative history on why that number. It certainly is one that bears a relevance in a number of cultural traditions. But I think we all know that one 13-year-old is not the same as another in many households and there is a large age group between again 13 and 18 that we should be thinking about as well.

Mr. CÁRDENAS. How do we expect a 13-year-old to do, wade through this without parental consent or somebody, an adult helping them?

Ms. O'CONNOR. I totally agree. I think kids, teenagers, and grownups in this country deserve greater supports and protections around their personal data online and off.

Mr. CÁRDENAS. I think it would be naive for us to believe that there isn't a motivation out there with the largest corporations in the world and getting more dominant and larger for them not to look at our children as consumers. If you look at the bandwidth of a consumer power of a teenager and a 20-some-year-old and a 30-some-year-old, et cetera, there is tremendous motivation for individuals to abuse the information of our children. And I think it is important that—thank you for the confidence that you gave that you believe that Congress is actually going to pass something. I hope that we do. Thank you for that confidence. I yield back.

Ms. SCHAKOWSKY. And now I yield 5 minutes to Mr. Gianforte.

Mr. GIANFORTE. Thank you. And, first, I would like to thank the chairwoman and ranking member for welcoming me to this committee. Thank you. I look forward to serving and I am encouraged by the conversation today. I think there is some good bipartisan common ground here to find solutions.

The internet has removed geographic barriers from many of our rural areas that previously prevented small companies in rural towns from competing globally. Concerns about data misuse are warranted, but creating an overburdensome regulatory environment would have devastating effects for this coming new prosperity we are seeing in rural America.

I think we all agree and we have heard it in the testimony today that consumer data must be secured and that we need more transparency and accountability in all of our practices and we need a national standard. Our job is to find a balance between these overly prescriptive laws like GDPR and versus a patchwork of 50 different laws in different States. Trying to comply with either would devastate small businesses. We have heard that in the testimony today, while increasing market share for some of the largest companies we see and this is what has caused the concern.

The burdensome top down approach taken by GDPR can stifle innovation and lead to less information simply because it is too costly to comply. It is imperative then we adopt one national standard and that clearly defines the responsibilities of consumers and businesses and I think we have unanimity on the panel today, so I appreciate that. Consumer concerns over their data can be attributed back to a lack of transparency and misunderstanding of how their information is being collected and used. Bad actors should be punished. We have seen many of them pursued by the FTC and also through the loss of consumer confidence.

The market tends to enter in here. In our internet business my wife and I started in our home, over 15 years it grew to one of the top 100 websites in the world. We had about 8 million consumers a day and we were entrusted with the data for nearly 2,000 organizations around the world. Protecting customer data was paramount in our business. We knew that the safety of our customers' data which we protected in the cloud was the key to continued viability of our business. The stakes and the consequences could not have been higher. We had to protect our customer data or face going out of business. It is difficult to regulate a dynamic industry and hastily rushing to draft legislation could have more unintended consequences than solutions. We have seen that in GDPR and in the California regs. As debate over consumer protection continues we should pursue one national standard that increases transparency and accountability while protecting small business and innovation.

I have a couple of questions. Dr. Layton, with all of this in mind and in light of the light regulatory touch we have taken in the U.S., historically, can you please discuss what you believe are the best way to guard against entrenching larger companies and disadvantaging smaller business?

Dr. LAYTON. Well, in two words, permissionless innovation. I mean, I think that that has been one of the most important things about our economy, was that we allowed companies to try. Just as you, yourself, you didn't have to—I doubt that you went to Washington and said, "May I try this website?" and you just got going.

Mr. GIANFORTE. Yes. OK, thank you.

And, Mr. Grimaldi, we heard from Ms. O'Connor and her litany of 260 applications—very impressive—and the intractability of complying with them all. And in your testimony I thought it was very helpful you recommended moving from these disclosures and checkboxes to prohibited practices. Can you give us a couple of examples of prohibited practices that you would put on that list if we were to draft legislation with that approach?

Mr. GRIMALDI. Sure. Thank you, Congressman. I think Ms. Collins-Dexter has an unbelievable list in her testimony. Eligibility, improper targeting because of eligibility, and discrimination, the use of sensitive information which would need to be defined, we have spoken a lot about it today that consumers don't anticipate and would never want to share and would never want to be used. I would say even if it is synonymized and not linked to their personal data along the lines of healthcare providers or addresses, et cetera. I think that is all important.

Mr. GIANFORTE. Do we need to differentiate between the types of data that is being collected and how would you suggest we do that?

Mr. GRIMALDI. Absolutely. I think that is—again, Europe should not dictate what our national law should be. I don't think one State should either. I think this body and the Senate is the best representation of what consumer sentiment is around these issues. My industry needs trust or else we don't have people logging on to our websites, we don't have people clicking on our ads. The whole internet economy is built on that. These are the things, these are the important conversations.

Mr. GIANFORTE. OK, thank you. I want to thank the panel for your testimony today. It is very helpful. And with that I yield back.

Ms. SCHAKOWSKY. And now a belated happy birthday, and I call for 5 minutes on Mr. Soto.

Mr. SOTO. Thank you, Madam Chairwoman. I believe most Americans have a basic understanding that their personal data is being used, but there are certain expectations of privacy that I think are reasonable for users to be able to have throughout the United States that their personal data be kept secure and not be stolen in a cyber breach, that their health data be protected so that it couldn't just be acquired without their permission, or that we avoid a society where government monitors all of our data in some Big Brother-type of situation that we are seeing now in China and in Russia.

You know, we have heard some complaints about States getting involved in this and the Supreme Court has gotten involved in it, which I will get into in a second. Really, the internet is a part of interstate commerce, but it is this committee's lack of action in legislating that has created this vacuum for States to act.

First, I want to just point out that the Supreme Court has already stated we some right to privacy for our personal data. In the recent *Carpenter v. United States* case, they at least applied the Fourth Amendment to say that government cannot get personal data from our cell phones without a warrant and I wouldn't be surprised by a 5–4 majority or more that that is extended to other rights. So the Supreme Court is already acting. States have already stepped up.

There has been a lot of talk, first, about a duty of care. That has mostly been in the purview of academia, but it is something that we ought to consider, cybersecurity protections, proper use of data consistent with disclosures, and handling requests and complaints for use of data. A second big issue we saw Delaware tackle with requiring privacy policies to be conspicuously available on websites. I don't think that is much to ask since we have that for a lot of contracts.

And then, thirdly, is really sort of the big question on privacy in general. California passed the Consumer Privacy Act of 2018 where there is a right to request businesses to disclose data collected, right to request businesses delete personal information, and then a right to opt-out without being discriminated against. And I think that is the multitrillion-dollar question in the room today and that is where I want to start by asking our panel.

Starting with Ms. O'Connor, do you think that you should be able to opt out of these sites' ability to collect data without being discriminated against, basically denied use of service?

Ms. O'CONNOR. Certainly. And as I mentioned before, there is a primary purpose and a primary data collection for the transaction. So to send me the book or the yellow sweater you have to know my address, but I do think individual consumers deserve more, not only agency but control over their data and the data lifecycle to access, correct, and delete data if they want to as well.

Mr. SOTO. Thank you for your input.

And, Ms. Collins-Dexter, do you think you should be able to opt out without discrimination?

Ms. COLLINS-DEXTER. Yes. I think opt-in forces—well, rather, I think when you set an opt-in framework it forces companies to make the case for why data is needed for desired use and why consumers should consent to that. I think, however, even in an opt-in framework, I think as we have heard examples over the day, companies will do all sorts of tricky things to get consumers to consent to things that they want to do.

And so I think legislation has to really move beyond a choice framework and really focus on prohibiting harmful use of data, establishing baseline norms and obligations such as data minimization and purpose limitation.

Mr. SOTO. Thank you.

And turning to innovation on this aspect, Ms. Zheng, do you think it would be a viable alternative that people can charge a user fee should they want to opt out of data collection? Would that still embrace the kind of innovation that you have been talking about?

Ms. ZHENG. Thank you for that question. I think if the companies choose to do that or choose to adopt that approach that would make sense, but I am not sure that mandating it in statute would make any sense. It would certainly hurt innovation.

Mr. SOTO. And, Mr. Grimaldi, on this sort of choice should you be able to opt out without discrimination or would it be appropriate to potentially charge the user fee in the alternative or deny a service altogether?

Mr. GRIMALDI. Thanks, Congressman Soto, a couple things. We see that not in terms of data for shopping data, for other use, but we see that in terms of just the value of exchange on if you want to access a certain subscription website and view their content you have to pay a fee. That is that value exchange.

To your question of should you be able to opt out and not receive those services, I think that is another thing that needs serious contemplation, because I don't think a one-fits-all approach would work here, just in terms of that being a defined right and the massive disruption that could cause to websites large, small, Google, Amazon, a small yogurt shop. If you opt out of giving your data, can those companies survive? Are they monetizing it in a way that a consumer knows about that, has that policy in their face, or the opt-out mechanism in their face? We supply that, as I mentioned earlier, via a large multistakeholder regime.

So there are tools out there. Could they be stronger? I think that is a great question.

Mr. SOTO. Thanks. My time has expired.

Ms. SCHAKOWSKY. Now I am happy to yield to Congresswoman Matsui.

Ms. MATSUI. Thank you very much, Madam Chair. And I want to thank the panel for being here today. This has been a very enlightening discussion. And I just want to make a comment about the elephant in the room, although I don't really regard it that way. As you can tell I am from California and there has been a lot of comment about the California law.

But may I just say about California there has not been much action on the Federal front, we all know that. And California being California with its myriad of businesses both big and small and its diversity, we have rural areas, urban areas, and suburban areas and it is not something that—we are not a small State, we have a myriad of opinions. And we are also a very innovative State, the home of many of the large companies that actually testified last spring.

So I just will tell you this. There are ways that I know Mr. Grimaldi saying he is already working with the State of California, I think that is really very important, but I must say also that it is something to be considered that it is a State that is large enough to really be able enact a law but also to bring in many of the stakeholders too. So that is my piece on California.

I want to talk about advertising. Advertising supported models generate revenue through user provided data. Many platforms have broad statements that claim what is yours is yours, you own your content. I appreciate that. But I want to understand more about that. To me that means users ought to have some say about if, how, and when it is used.

But online platforms have an evolving set of rules for how partners can interact with the user content and how the platform may modify or adapt this content as it is distributed. The hearings this committee has held demonstrate that the real crux of the issue is how content is used and modified to develop assumptions and inferences about users to better target ads to the individual.

I want to ask, how should a Federal privacy law ensure consumers have a meaningful say about how their data is used even when that data has modified use to develop inferences supplemented by additional data or otherwise? And I will start with you, Ms. O'Connor.

Ms. O'CONNOR. Thank you so much for that question. We would believe that there should be limitations on the secondary use of data that you have provided for a particular service and obviously transparency around the operations of the company and their intended use. I think your question gets to the heart of the matter, which is that individuals do not want to be discriminated online or offline and they want to know how the decisions that are being made about them are affecting their daily lives.

So we would absolutely want to look at issues of discrimination again in the online-offline world based on the data that is collected and allow the individual greater agency and control over that data.

Ms. MATSUI. Thank you.

Now it has been noted that advertising is less concerned with identifying the individual, per se, than with the activity of the users to predict and infer consumer behavior. But I wonder if that is becoming a distinction without a difference even when user content isn't associated with that user's name, precise information can

and is gathered through metadata associated with messages or tweets. For instance, online platforms often are offered geospatial metadata that they provide by parsing messages for location names of interest including nicknames. This metadata could then be associated with other publicly available social media data to re-identify individuals.

Ms. O'Connor or Mr. Grimaldi, so even though advertising itself may not be considered with identifying the individual in the context of the Federal privacy law, how do we ensure data is not being used by others to do so?

Mr. Grimaldi, first.

Mr. GRIMALDI. Sure. Thank you, Ms. Matsui. And I think that those are very important questions that a potential, new, strong oversight regime would contemplate. A number of folks have mentioned the Federal Trade Commission. They have brought 500 cases or more on issues around these types. And while they are incredibly capable and very strong, they don't have the resources right now, I think, that would allow them to play a role in a massive part of the American economy.

So I think that that is up for discussion as to whether or not a new paradigm, the one that we are contemplating could bring new oversight and new enforcement and that is part of what we are discussing now. A moment ago I think it was Mr. Soto or Mr. Cárdenas mentioned the jurisprudence in the past around these issues. And I think it would—I was a staffer on this committee when long after the 1996 act was passed and there was much discussion about why that was never updated, why there was never momentum behind that to update it. And I think it is because getting in the way of innovation and getting in the way of consumers enjoying what they want and the services they are provided is a sticky thing. But in terms of more oversight and new powers to protect consumers, I think we are at a place right now where we need to seriously think about that and make it happen.

Ms. MATSUI. OK, thank you. I am out of time. I yield back.

Ms. SCHAKOWSKY. And next, also from California, Congressman McNerney.

Mr. MCNERNEY. There is a lot of us from California. Thank you.

Ms. MATSUI. Big State.

Mr. MCNERNEY. Thank you. I want to thank the witnesses for your perspectives on this. It is an important subject and it is complicated. It is not something you can get your hands around easily, so thank you very much.

My first question goes to all the witnesses and please just answer yes or no. Is it important that any law that we draft be able to adapt to technological innovation and advancements over time? Starting with Ms. Collins.

Ms. COLLINS-DEXTER. Yes.

Dr. LAYTON. Yes.

Ms. ZHENG. Absolutely, yes.

Mr. GRIMALDI. Yes.

Ms. O'CONNOR. Yes.

Mr. MCNERNEY. Unanimous. Well, that makes my point.

In order for comprehensive privacy laws created by this slow-moving Congress to meet the current challenges and to be able to

adopt the new circumstances, I believe it is critical that we give the FTC APA rulemaking authority for privacy and data security. I have called for this over time and I expect to see that in our policy.

My next question will go to Ms. Collins-Dexter. When Facebook CEO testified before this committee I asked him if I could download all of my data that Facebook had and he said an unqualified yes. And then later in the hearing after being advised by his staff that that wasn't correct he corrected his statement. Now, Ms. Collins-Dexter, if a CEO of a major company that deals in data, that is their business, isn't sure what data they make available to its users, can we have any confidence at all that these companies will actually make their data available to users when requested?

Ms. COLLINS-DEXTER. No, we can't.

Mr. MCNERNEY. Well, good. And clearly it is important that the comprehensive data privacy legislation grant consumers the right to access their data and to correct it if it is wrong.

You are not raising your hand to make a statement, I don't think.

Dr. LAYTON. No, I agree.

Mr. MCNERNEY. Thank you.

Again Ms. Collins-Dexter, can you explain the risks that location tracking poses for low-income Americans like so many of my constituents?

Ms. COLLINS-DEXTER. Yes. I also, if I may, want to sort of take us back again. I think there has been like a lot of conversation around patchwork legislation. And while I think there is certainly issues with GDPR, there is improvements to be made with California legislation.

I think one thing that I think came up in the testimony with Mark Zuckerberg that I think we should identify as really part of the issue of coming here is really an issue around tech monopolies and how they are consolidating power. And so I really think that it is important for us to maintain that even as we are looking at the ways in which they are collecting innocuous data points such as geolocation in order to ascertain things around race and come and use that as an opportunity to use predatory payday advertising, junk food marketing, and all sorts of sort of harmful advertising targeted at communities in different locations.

Mr. MCNERNEY. Thanks for that comment. Well, I think it is important that we limit the use of data location information and that is something that I will be working with Members across the aisle on.

Again Ms. Collins-Dexter, in your written testimony you mention that algorithms work as kind of a black box to drive exclusionary practices and you need to raise, need to ensure that fairness in automated decisions. What do you think are some of the challenges that companies face in this today?

Ms. COLLINS-DEXTER. Yes. I think part of what we are looking at or thinking about is this proposition of kind of garbage in-garbage out, right. And so I think there is a lot of presumptions that algorithms can't be biased or that tech is neutral. And what we find is history, a long, you know, history of systemic inequities are actually being and put in from data points and then replicating models of discrimination free from accountability.

And so I think, you know, one of the things that we want to look at is kind of the algorithm, distribution of advertisements related explicitly to education, employment, and housing opportunities, algorithmic distribution of political advertisements in communications, and algorithmic determinations of product prices and same-day shipping. These are examples of some of the things in which I think we need to see more intelligence and information on.

Mr. MCNERNEY. Thank you.

Finally, Ms. O'Connor, I am worried about data security as well as data privacy. Would you agree with that?

Ms. O'CONNOR. Yes, sir.

Mr. MCNERNEY. What is the relationship between privacy and security?

Ms. O'CONNOR. They are inexplicably linked. They are two sides of the same coin. In our draft proposal we copy some of Congresswoman Schakowsky's language about thresholds and best practices and it is an essential part of a privacy program for any company large or small.

Mr. MCNERNEY. Thank you. And I just want to say I was shocked by your earlier statement, Ms. Collins-Dexter, that discriminatory technology is lucrative to identify ethnicity. In other words it is a lucrative technology used nefariously. Thank you. I yield back.

Ms. SCHAKOWSKY. And now Mr. O'Halleran for 5 minutes, you are recognized.

Mr. O'HALLERAN. Thank you, Madam Chair. And I thank too the witnesses also that are appearing before us today.

You know, I am all for a national policy, but it has to be balanced. And it has to be balanced for the good of the people of America and their privacy. We have to recognize that there is, you know, not only are these changing times but the speed at which technology is changing has to be taken into account. I was a former investigator and I have to tell you, I would love to be an investigator in these times because of the speed of information that I could get that used to take me maybe a month to get, I could get in minutes maybe.

So we have to be very concerned about these issues. And this is a national dialogue on how to enhance the data privacy of consumers. This is a debate that it is important not only to the people in my district in Arizona, but the American people. I have to kind of thank California and thank Europe for getting us pushed. Do I agree with necessarily about what they want to do? No. But do I think it has allowed us to be pushed in the right direction in a timely fashion? Yes, we should have done this much sooner.

As members of this committee across the aisle, we must take seriously our duty to closely examine how to ensure consumer privacy remains protected in today's increasingly connected global economy.

Ms. Zheng, as you know my rural district in Arizona is home to many small businesses who constantly strive to compete in a modernizing economy and internet ecosystem. Under current law, the Federal Trade Commission serves as the primary enforcer for internet privacy as prescribed by the FTC Act. Taking into consideration the FTC's mandate to combat unfair and disruptive trade

practices, deceptive trade practices against consumers, what privacy framework do you see as striking the right balance between protecting the rights of consumers and helping ensure regulatory certainty for small businesses?

Ms. ZHENG. Thank you for that question, Congressman. I would note that in a number of laws as well as legislative proposals, lawmakers have contemplated an exception for small or medium-sized businesses. I assume that is something that this body will also contemplate. You know, as the Business Roundtable we do represent large American companies, but many of our companies do business with small companies as their clients or as their suppliers so we certainly care about the well-being of the small business community.

I think, you know, there are different types of thresholds you could look to in considering a possible small business exception including potentially the number of records held or the annual revenue. But I am not certain that the Business Roundtable is really the best organization to pontificate on what specifically that threshold ought to be.

Mr. O'HALLERAN. And probably the reason for my question is because I want to see that there is a protection for businesses across the entire spectrum, not just for those with large business concerns.

Ms. O'Connor, in your testimony you state that existing privacy regimes rely too heavily on the concept of notice and consent which you state place an untenable burden on consumers. As we all know, consumers often overlook the extremely dense language—here I am—in user agreements and simply accept in order to use internet applications and services.

Under any new consumer privacy statute how could privacy notices be simplified for consumers whether they are technologically experts or novices to better and more meaningfully understand how their information is being stored, used, and, if applicable, shared after accepting privacy agreements? And I will say I believe the chairwoman was correct in her stack, it is probably a much bigger stack. And we have to design something that works for the American people. Please.

Ms. O'CONNOR. Thank you, sir. That is exactly right. The number of hours and the number of words we would all have to read on a daily or weekly or monthly basis to stay up-to-date on the choices we are making online and off about how our data flows are staggering and overwhelming to any busy consumer. I think there should be things that are in bounds, again for the furtherance of the transaction, so the primary purpose of the deal.

There should be things that are simply out of bounds like taking biometrics for purposes that are far afield from the primary purpose of the transaction, and then you could limit notices to that middle ground of things that are less clear but that consumers might want that are related to the transactions that they have at hand or their relationship with the company. They definitely need to be shorter, clearer, and more to the point. But notice and choice alone do not get us where we need to go.

Mr. O'HALLERAN. Thank you, and I yield. Thank you, Madam Chair.

Ms. SCHAKOWSKY. Now I am happy to yield to my colleague from Illinois, Mr. Rush.

Mr. RUSH. I certainly want to thank you, Madam Chair, and I want to thank all the witnesses who have appeared before this subcommittee today. I chaired this subcommittee back in 2007. I introduced a data bill back in 2007, and we are still here today discussing data and data security and a data bill. And I hope that under this current chairman that we are able to finally come up with a bipartisan bill and that will pass in Congress and then the President will sign. I certainly look forward to it and I have been pretty patient about it.

I reintroduced my data protection, data privacy bill, H.R. 1282, that had one provision that dealt with this specter of data brokers. And I just wanted to know am I off-base, Ms. Collins? Am I off-base trying to rein in this specter of data brokers? How big is that problem and as it relates to protection of consumers' data?

Ms. COLLINS-DEXTER. Yes. I think that you are right to be concerned. I think there is like so much work we have to do. I think one of the things that I tried to articulate in my comments I think is super important is that 50 years ago as a country we made a sort of social, legislative, and legal contract that is that certain things would no longer be accepted in our society. Kids being turned away from Woolworth's counter was not acceptable. People hanging signs that said no Jews, dogs or blacks allowed were no longer acceptable. And we didn't throw our hands up at that time and say don't go to that restaurant, right. We took an ethical and moral stance.

And not just that, it was about knowing that if we could compete globally and thrive economically we had to ensure that we had more taxpaying members of our community, more people able to have opportunity and be economically mobile. And so part of what we are looking at with this like privacy legislation is basically looking at stopping Jim Crow online. It is around simply bringing, you know, looking at our online activities and ensuring that there is—that those same laws that we created 50 years ago to prevent discrimination apply to what we do online.

Mr. RUSH. Thank you.

Ms. O'Connor, what should we do to regulate data brokers?

Ms. O'CONNOR. Thank you, sir. And I think underpinning so many of the questions today is the issue of opaque or surreptitious surveillance or data collection. And that is the position again, and I just want to associate myself with Ms. Collins-Dexter because she is so right that these are issues of fairness, of transparency, of accountability, and of equality for all Americans.

Data brokers really came up because of the Fair Housing Act and the Equal Opportunity Act and the fundamentals of providing fair credit to all Americans. They served at that time a purpose. Right now the opaque and surreptitious behind-the-scenes data collection by third parties that Americans do not understand is fundamentally untenable going forward.

So, and I think the CEO of one of those companies is actually directly across the hall right now, so maybe we could go ask him some of these questions. But they do serve a purpose. And to the

previous comments, we need to reform, we need transparency, and we need greater control and accountability over these third parties.

Mr. RUSH. In your testimony you discuss how the CDT's draft legislation—well, I quote you, “would direct the FTC to promulgate rules addressing unfair advertising practices, particularly those that result in unlawful discrimination in violation of civil rights law.” Describe for this committee what should these rules look like?

Ms. O'CONNOR. There are good laws on the books as we all know about unfair discrimination and what that looks like in the offline world. However, intimate and immutable and real-time decisions can be made about us in the online world even prior to knowing who we are based on inferences, based on patterns of surfing and habits. We would simply want to make sure that each individual's world view is not prescribed and limited by judgments that are made about them by companies that they are not aware of. That a child in one part of the country is not seeing ads for educational opportunities or a grownup is not seeing credit opportunities that another person is being served based on judgments companies are making about them without their knowledge.

Mr. RUSH. Thank you, Madam Chair. I yield back.

Ms. SCHAKOWSKY. Now it is my pleasure—last but not least—to call on Representative Kelly, also from Illinois.

Ms. KELLY. Madam Chair, Illinois is holding it down for you or with you. Thank you, Madam Chair, for holding this hearing today.

As we have heard, repeated news stories about breaches and data collection malpractice have shown that it is time for Federal privacy legislation. As the founder of the Tech Accountability Caucus, I want to follow up on the discussion of use of limitations.

Ms. O'Connor, in your testimony you discuss two buckets of use limitations, the first of which you refer to as unfair data practices. The CDT draft legislation prohibits secondary uses of certain sensitive data like biometric information and health information. Can you clarify something for me? Other than the specific exceptions listed, is it your intention in the draft that these seven unfair categories are just not permitted?

Ms. O'CONNOR. That is correct, ma'am, that the secondary use of those categories of data would not be permitted. Each individual would have to enter into a separate contract or agreement for a separate service or a separate device.

Ms. KELLY. I know we talked about during this hearing about opting in and all of that, but a company cannot even seek opt-in consent for their uses; is that correct?

Ms. O'CONNOR. It would have to be an entirely separate transaction. That is right.

Ms. KELLY. OK. How did you decide the types of data that necessitated the extra protections?

Ms. O'CONNOR. The Center for Democracy & Technology worked over the last several years and we have stood for and been in favor of omnibus Federal privacy legislation for the entire 25 years of CDT's existence. But we have re-energized this debate internally and worked with academics across this country and really around the world, business partners, other advocates in civil society and looked at the research and the consumer polling, the consumer re-

search in this area, and that is where we ended up with the list that we created.

Ms. KELLY. OK, thank you. And to the panel, are there certain types of data that shouldn't be collected or used at all? We can just run down from Ms. Collins-Dexter.

Ms. COLLINS-DEXTER. Yes, I think there is certain pieces of like personal identifying data, geolocation, things like that that I think should not be collected and kept in use.

Ms. KELLY. Dr. Layton? Just your opinion, are they any types of data that shouldn't be used at all or collected?

Ms. ZHENG. Thank you, Congresswoman, for that question. I think that the question deserves a little bit of nuance. What we are talking about here is, is there data that deserves an opt-in consent standard and I think the answer to that is likely yes. For example, a precise geolocation data, the FTC's current guidance right now is you acquire opt-in consent for precise geolocation data.

What the Business Roundtable proposal recognizes is that there are sensitive categories of data that do absolutely deserve heightened protections and obligations including potentially opt-in consent.

Ms. KELLY. Thank you.

Mr. GRIMALDI. Congresswoman, I would chime in by saying in order for the entire online ecosystem to work there has to be data to render a website to provide services, et cetera. And so in addition to some of the prohibited pieces that we have heard today that we all agree on, how do we expand that list to include other things in the marketplace that as my co-panelists have mentioned are just getting such blowback or are just on their face too personal, too off limits to be used by our companies, by other companies, I think that is important. And we need to make sure that the value that consumers are getting from their online experience can still be reaped even as we expand that list and we would love to work with you on that.

Dr. LAYTON. Congresswoman, I just wanted to come back. I didn't want to take a position on this because I know, I actually know of important health and academic studies that under today's circumstances in the GDPR the data could not be collected. But data that had been collected in the past has been used today to make very important conclusions for health questions. So I only urge—I just want to put a note of caution, I understand that we have these concerns. But we don't necessarily know in the future how the data may be available.

So I would tend to fall on the side of where we can identify that it is sensitive and have a higher standard, but not necessarily to outlaw it altogether. I am just concerned about the future because I have seen these studies that, you know, going forward we won't be able to do these important health outcome studies in the EU.

Ms. KELLY. OK, thank you. Anything else? I will yield back the balance of my time. Thank you.

Ms. SCHAKOWSKY. So, in closing, first let me request unanimous consent to enter the following documents into the record: 1) Public Citizen Framework for Privacy and Digital Rights for All; 2) a letter from the Americans for Prosperity; 3) a letter from Computer and Communications Industry Association; 4) a letter from the

ACLU and 42 other civil rights organizations; 5) a letter from Main Street Association; 6) a letter from Consumer Technology Association; 7) Engine consumer privacy comments; 8) letter from Engine; 9) a letter from American Bankers Association; 10) the NRF letter; 11) NRF comments; 12) Electronic Transactions Association letter; 13) 21st Century Privacy Coalition letter; 14) ACA International letter; 15) Representative Eshoo's opening statement for the record. You can see the kind of broad spread interest.

I want to thank our ranking member, the staff that worked so hard on all of this, thank you, and especially our witnesses for your participation today in this very first hearing of the session dealing with this issue of data privacy which is clearly going to go forward. I encourage you to also keep in touch as we move forward. We welcome your input.

I remind Members that pursuant to committee rules they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared. I ask each witness to respond promptly to any such requests that you may receive.

Oh, there is more. OK. So we will have a letter from the American Action Forum to put in the record, a letter from the Council for Citizens Against Government Waste, a letter from consumer tech—oh, I see—a letter from the Coalition for Secure Transparent Internet, a letter from R Street Institute, a letter from United States Chamber of Commerce, a letter from Digital Liberty, a letter from the Internet Association, DOJ Cyber Digital Task Force, a letter from Google.

Is that it? There is more? OK, a lot of interest. OK. Still, I had the Public Citizen, I think. But Public Citizen Framework for Privacy and Digital Rights for All, the Electronic Transaction Association letter, the letter from the National Association of Mutual Insurance Companies, a letter from Information Technology and Innovation Foundation, and along with the others I ask unanimous consent to put these in the record. So ordered.

[The information appears at the conclusion of the hearing.]¹

Ms. SCHAKOWSKY. And now, I think, at this time the subcommittee is adjourned.

[Whereupon, at 12:51 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. ANNA G. ESHOO

I thank Chairwoman Jan Schakowsky for holding today's hearing and for allowing me to waive on to the Subcommittee on Consumer Protection and Commerce for this hearing.

Three important events set the table for our debate about online privacy. In March 2018, we learned that Cambridge Analytica abused Facebook data to harm our democracy. In May 2018, the European Union's General Data Protection Regulation went into effect. And in June 2018, then-Governor Jerry Brown signed into law the California Consumer Privacy Act. These three events have created the context within which I'm hopeful that Congress may be able to pass privacy legislation to protect all Americans. We should keep the lessons of each of these events in mind as we debate any privacy legislation.

¹The Information Technology and Innovation Foundation letter has been retained in committee files and also is available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108942>.

I have long called for protecting users' privacy online, and I reiterate my commitment to ensuring Congress passes strong and enforceable privacy legislation. However, not all privacy proposals are equal. Strengthening disclosures and simply expanding our "notice and consent" regime would be woefully insufficient for protecting users' privacy. We must shift the burden of privacy away from consumers who do not—and could not possibly—read hundreds of privacy policies that each run thousands of words long. A Federal law should require that companies minimize collection of personal data, give users access to and control of their data, eliminate problematic types of third-party data exchange, and institute safeguards to secure user data.

Further, too many people are calling for preemption when we haven't even agreed on the contours of what the law should include. As Congress debates national privacy standards, it should take care not to undermine California's groundbreaking privacy law. Instead, Congress should pass baseline privacy protections that bring the same—or stronger—safeguards to all Americans.

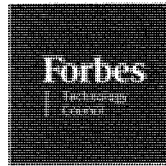
I represent much of Silicon Valley, and yes that includes some of the large tech companies that are at the center of the problems privacy legislation aims to solve. I also represent a thriving startup ecosystem. In my district, Y Combinator, the most successful startup accelerator in the world, has funded nearly 2,000 startups since 2005. These startups should be seen as part of the solution. Congress should consider proposals, such as data portability, that support privacy by encouraging competition.

Nearly every stakeholder is calling for a Federal privacy law. I'm hopeful that now is the time we will be able to pass something that truly protects Americans online.

<https://www.forbes.com/sites/forbestechcouncil/2019/01/15/2019-data-privacy-wish-list-moving-from-compliance-to-concern/#43f9caae2493>

Jan 15, 2019, 08:45am

2019 Data Privacy Wish List: Moving From Compliance To Concern



Ameesh Divatia Forbes Councils
Forbes Technology Council CommunityVoice

Post written by Ameesh Divatia

Ameesh Divatia is Co-Founder and CEO of [Baffle, Inc.](#), with a proven track record of turning innovative ideas into successful businesses.

For virtually every business, the last and first (calendar) quarters are filled with reflection and planning — for revenue, services, operations, budgeting and, of course, privacy and security. Throughout the year, I've spent a lot of time in my column examining emerging trends, both slow and rapid, in data privacy and security. As you're completing those spreadsheets and presentations, including the annual budgetary ask, I thought it would be useful to build upon those insights and look at what to prepare for this year.

Data Privacy And Protection Laws

The General Data Protection Regulation is now in full effect to protect the privacy of European Union citizens. The [California Consumer Privacy Act](#) passed in June 2018 and goes into effect in January 2020. New York has cybersecurity regulations specifically for [financial institutions](#). Work in Brazil? It has passed [one](#) as well. It's a messy landslide of different laws that can keep your legal and compliance teams running in circles.

Don't get me wrong: increased privacy protection laws are good and badly needed. However, virtually borderless internet and cloud initiatives make legal lines harder to identify, correlate and combine. Also, privacy regulations are not specifying how the data is to be protected. All they say is that if cleartext data is lost, it is mandatory to notify the affected parties and the regulators about that breach. Organizations can easily find themselves ping-ponging between compliance rules, and as I've said in the past, just checking compliance boxes has proven time and time again to be a failed security — and now privacy — strategy.

A Move From Privacy 'Compliance' to 'Concern and Care'

Organizations need to significantly shift their mindset about data privacy. I've argued that it starts with the appointment of a data protection officer and then goes from a compliance mindset and approach to one of data protection and stewardship. Companies argue that they need the data and they need to gather it aggressively in order to determine its value with analytics. However, this approach presents a Catch-22. The popular argument that we should be more careful with customer data is the new oil of the 21st century. It's not just about compliance anymore, but rather a philosophy that treats data with extreme care and with prevention of data breaches in mind.

Amplify Automation And Monitoring

Despite the advances (or hype, but that's for another column) in artificial intelligence and machine learning, humans still run businesses. Even with the best intentions, human beings make mistakes, which helps explain why phishing still remains such an effective tactic. They may go into a project with all the care in the world, but they still leave doors unlocked and create any number of errors that expose data.

Technology researchers at [Gartner, Inc.](#) have noted that security detection and response — rather than just preventative measures — is now a top priority for enterprises. With a worldwide shortage of nearly one million security professionals, we must automate routine processes amplify the impact of trained humans. Gartner [predicts](#) that by 2021, automation will be heavily weighted by one-fifth of all security buyers.

Reexamine Third-Party Partners And Their Data Access

Corporate walls have become increasingly transparent, and are not just confined to your full-time employees. Two years ago, [half](#) -- yes, half -- of all organizations experienced a data breach because of a business vendor or associate. While this may be getting better thanks to new privacy legislation and advances in encryption and other security solutions, the percentage of breaches still remains high.

In healthcare — a business ecosystem entrenched in a complicated mesh of third-party providers — there's some action underway. In August 2018, CISOs at some of the largest health providers formed a [consortium](#) to help address third-party risk. Other industries should also find a common set of strict data care policies and technologies that must be followed, rather than operating on a case-by-case or contract-by-contract basis.

But there's no need to wait for a consortium or a compliance standard to do the right thing with privacy and security of data. Your customers demand better care of their data. Use your 2019 planning to establish best practice guidelines for your organization, and then share those policies (and lessons learned) with your industry peers. But most importantly, shift your mindset to one of extreme concern and care for customer information and privacy — not just regulatory compliance.

[Forbes Technology Council](#) is an invitation-only community for world-class CIOs, CTOs and technology executives. [Do I qualify?](#)



[Ameesh Divatia](#) Forbes Councils

Ameesh Divatia is Co-Founder & CEO of [Baffle, Inc.](#), with a proven track record of turning innovative ideas into successful businesses.



[Forbes Technology Council](#) CommunityVoice

Forbes Technology Council is an invitation-only, fee-based organization comprised of leading CIOs, CTOs and technology executives. Find out if you qualify at [forbestechcouncil.com](#). Questions about an article? Email feedback@forbescouncils.com.

THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL RIGHTS IN THE UNITED STATES

The United States confronts a crisis. Digital giants invade our private lives, spy on our families, and gather our most intimate facts for profit. Bad actors, foreign and domestic, target the personal data gathered by U.S. firms, including our bank details, email messages, and Social Security Numbers.

Our privacy laws are decades out of date. We urgently need a new approach to privacy protection. We must update federal laws and create a data protection agency specifically tasked with safeguarding the privacy of Americans. The time is now.

1. ENACT BASELINE FEDERAL LEGISLATION

We call for federal baseline legislation that ensures a basic level of protection for all individuals in the United States. We oppose the preemption of stronger state laws. U.S. privacy laws typically establish a floor and not a ceiling so that states can afford protections they deem appropriate for their citizens and be “laboratories of democracy,” innovating protections to keep up with rapidly changing technology.

2. ENFORCE FAIR INFORMATION PRACTICES (FIPS)

Baseline federal legislation should be built on a familiar privacy framework, such as the original U.S. Code of Fair Information Practices and the widely followed OECD Privacy Guidelines. These frameworks create obligations for companies that collect personal data and rights for individuals. Core principles include:

- | | |
|---|--------------------------------|
| • Transparency about business practices | • Access and correction rights |
| • Data collection and use limitations | • Accountability |
| • Data minimization and deletion | • Data accuracy |
| • Purpose specification | • Confidentiality/security |

“Personal data” should be broadly defined to include information that identifies, or could identify, a particular person, including aggregate and de-identified data.

Federal law should also:

- Establish limits on the collection, use and disclosure of sensitive personal data,
- Establish enhanced limits on the collection, use and disclosure of data of children and teens,
- Regulate consumer scoring and other business practices that diminish people’s life chances, and
- Prohibit or prevent manipulative marketing practices.

3. ESTABLISH A DATA PROTECTION AGENCY

Many democratic nations have a dedicated data protection agency with independent authority and enforcement capabilities. While the Federal Trade Commission (FTC) helps to safeguard consumers and promote competition, it is not a data protection agency. The FTC lacks rulemaking authority. The agency has failed to enforce the orders it has established. The US needs a federal agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges. The agency should also examine the social, ethical, and economic impacts of high-risk data processing and oversee impact-assessment obligations. Federal law must establish a data protection agency with resources, rulemaking authority and effective enforcement powers.

4. ENSURE ROBUST ENFORCEMENT

Robust enforcement is critical for effective privacy protection. Arbitration clauses do not protect consumers and permit dangerous business practices to continue. If a company violates federal privacy law, consumers must be able to pursue a private right of action that provides meaningful redress without a showing of additional harm. Statutory damages are an essential element of an effective privacy law. Robust enforcement also requires independent action by State Attorneys General.

5. ESTABLISH ALGORITHMIC GOVERNANCE TO ADVANCE FAIR AND JUST DATA PRACTICES

The use of secret algorithms based on individual data permeates our lives. Concerns about the fairness of automated decision-making are mounting as artificial intelligence is used to determine eligibility for jobs, housing, credit, insurance, and other life necessities. Bias and discrimination are often embedded in these systems yet there is no accountability for their impact. All individuals should have the right to know the basis of an automated decision that concerns them. And there must be independent accountability for automated decisions. Protecting algorithms as a trade secret overprotects intellectual property and creates a barrier to due process. Trade agreements should uphold algorithmic transparency. Algorithmic transparency is central to algorithmic accountability.

6. PROHIBIT “TAKE IT OR LEAVE IT” TERMS

Individuals cannot have meaningful control of their personal data if the terms of service require them to waive their privacy rights. Furthermore, requiring individuals to pay more or receive lower quality goods or services if they do not waive their privacy rights is unfair and discriminates against those with less means. Federal law should require that consent, where appropriate, is meaningful, informed, and revocable, and should prohibit “pay-for-privacy provisions” or “take-it-or leave it” terms of service.

7. PROMOTE PRIVACY INNOVATION

Federal law should require innovative approaches to privacy and security, including strong encryption, robust techniques for deidentification and anonymization, and privacy enhancing techniques that minimize or eliminate the collection and disclosure of personal data, and make privacy by design an affirmative obligation. The consolidation of personal data with a small group of firms has stifled innovation and competition. Antitrust enforcement agencies should consider privacy interests in merger review. Mergers that fail to protect the privacy of consumers should be rejected.

8. LIMIT GOVERNMENT ACCESS TO PERSONAL DATA

Personal data held by companies are often sought by government agencies for law enforcement purposes. We do not object to the disclosure of specific records that are required for legitimate criminal investigations and obtained through an appropriate judicial procedure. However, there should be a clear standard in a privacy law for such disclosure. U.S. companies cannot disclose user data in bulk to government agencies.

Signed,

*Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Digital Democracy
Center for Media Justice
Color of Change*

*Consumer Action
Consumer Federation of America
Defending Rights & Dissent
Electronic Privacy Information Center
Media Alliance*

*Parent Coalition for Student Privacy
Privacy Rights Clearinghouse
Privacy Times
Public Citizen
Stop Online Violence Against Women
U.S. PIRG*



February 26, 2019

Subcommittee Chairman Schakowsky and members of the Subcommittee on Consumer Protection and Commerce:

On behalf of more than 3.2 million Americans for Prosperity activists across all 50 states, I thank you for holding this important hearing today on consumer privacy. At AFP, we believe that Congress can protect consumer privacy without hampering the technological innovation that has enhanced our nation's economy and benefitted consumers over the past decades.

Congress has an opportunity to protect consumer privacy while ensuring Americans continue leading the way in developing cutting-edge technology. While the impact of new technologies has been overwhelmingly positive for the public, they also pose new challenges for policymakers to solve. However, heavy-handed regulatory measures are not an effective solution. Instead, they create new barriers to innovation while doing little to protect consumers. The net result of such innovation-blocking regulation is to leave consumers worse off in the long run.

We urge the subcommittee to adopt the following principles while crafting privacy legislation. First, that privacy legislation should focus on addressing practices that harm consumers. Second, that it maintains a clear distinction between privacy and data security. Third, that the legislation recognize the practical and legal complexities of using an ownership metaphor for all data. Finally, the committee should not grant the Federal Trade Commission broad rulemaking authority. Instead, it should clarify the FTC's existing authority to combat unfair and deceptive practices. We have enclosed two articles that further articulate our principles for the committee to review.

We stand ready to work with any and all lawmakers who will make this issue a priority. We look forward to working with this committee to implement solutions that will protect the privacy of consumers and maintain American innovation.

Sincerely,

Brent Gardner
Chief Government Affairs Officer
Americans for Prosperity

Through broad-based grassroots outreach, *Americans for Prosperity (AFP)* is driving long-term solutions to the country's biggest problems. AFP activists engage friends and neighbors on key issues and encourage them to take an active role in building a culture of mutual benefit, where people succeed by helping one another. AFP recruits and unites activists in 35 states behind a common goal of advancing policies that will help people improve their lives.



**Computer & Communications
Industry Association**
Tech Advocacy Since 1972

February 25, 2019

The Honorable Janice D. Schakowsky
Chairwoman
Subcommittee on Consumer Protection & Commerce
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection & Commerce
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairwoman Schakowsky and Ranking Member McMorris Rodgers:

On behalf of the Computer & Communications Industry Association (CCIA), I write regarding the Subcommittee's hearing on "Protecting Consumer Privacy in the Era of Big Data." CCIA is an international association that represents companies of all sizes in the high technology products and services sectors, including in computer hardware and software, electronic commerce, telecommunications, and Internet products and services.¹

This hearing is timely, and CCIA appreciates the Subcommittee's efforts to examine these critical issues. Public attention to the subject of data protection, risks of the emergence of an unworkable 50-state patchwork of inconsistent regulations, and pressures from international privacy frameworks, such as the General Data Protection Regulation (GDPR), have underlined the need for strong and consistent rules of the road for the treatment of consumer information. In November 2018, CCIA issued its "Privacy Principles: A New Framework for Protecting Data and Promoting Innovation," setting out principles for federal action that would ensure that data is handled responsibly and transparently while also ensuring that individuals can benefit from innovation and new technologies.² These principles are attached for your reference. A growing number of companies, trade associations, and civil society groups also support the development of strong, baseline federal privacy legislation in order to promote a sustainable digital economy that will drive U.S. innovation and competitiveness. CCIA has created a chart organizing various industry proposals and highlighting the key issue areas they have addressed.³

¹ CCIA's members employ more than 750,000 workers and generate annual revenues in excess of \$540 billion. A full list of CCIA members is available at <https://www.ccianet.org/members>.

² *Privacy Principles: A New Framework for Protecting Data and Promoting Innovation*, Computer & Communications Industry Ass'n (Nov. 2018), http://www.ccianet.org/wp-content/uploads/2018/11/CCIA_Privacy_Principles.pdf.

³ See *Envisioning a Federal Baseline Privacy Framework*, Disruptive Competition Project (Feb. 25, 2019), <https://www.project-disco.org/privacy/022519-envisioning-federal-baseline-privacy-framework/>.

GAO Report

CCIA welcomes the Government Accountability Office's (GAO) recent privacy report to Chairman Pallone,⁴ which recommends that Congress "consider developing comprehensive legislation" on privacy and raises three issues for Congressional consideration. CCIA supports the thrust of the GAO report toward comprehensive, baseline federal legislation to protect consumer privacy without disrupting existing federal, sector-specific frameworks. However, legislation with a limited scope could undermine widely shared goals. The goal of baseline federal rules should be to ensure that individuals can expect consistent treatment of their personal information throughout the economy. Rather than artificially limiting new legislation to "Internet privacy," a new framework should apply to all organizations that collect and process personal information, including both online and offline companies, whether or not they have a direct commercial relationship with consumers. CCIA offers the following comments on three important questions posed by the GAO.

Which agency or agencies should have oversight?

Comprehensive baseline privacy legislation should be primarily enforced by the Federal Trade Commission (FTC) and extend uniformly to businesses and non-profit organizations. The FTC has experience and expertise in the data privacy and security context. The FTC's existing privacy authority allows it to bring enforcement actions against "unfair and deceptive acts and practices in commerce" and enforce a variety of sector-specific laws such as the Children's Online Privacy Protection Act (COPPA).⁵ The FTC may bring enforcement actions to require companies to take affirmative steps to remediate unlawful behavior. These actions have included mechanisms such as requiring the implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, and providing robust transparency and choice mechanisms to consumers.⁶

What authorities should a regulating agency have?

As the GAO report recommends, it is appropriate to consider granting APA-rulemaking authority to the FTC to implement a suitably specific baseline privacy law. It is also appropriate to consider whether the FTC should have the authority to issue civil penalties to first-time violators of that law. However, these proposals should not be the boundaries of the conversation over federal privacy authority.

Congress should evaluate whether State Attorneys General should be empowered to investigate when the FTC has declined to act. Congress should also provide the FTC with additional resources and staffing to conduct investigations, take enforcement actions, host workshops, issue public reports, and complete the necessary empirical studies to quantitatively evaluate the net consumer benefits and harms of particular

⁴ U.S. Gov't Accountability Office, GAO-19-52, Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility (Jan. 15, 2019), <https://www.gao.gov/assets/700/696437.pdf>.

⁵ 15 U.S.C. §§ 6501–6506.

⁶ *Privacy & Data Security Update: 2017*, Fed. Trade Comm'n (Jan. 18, 2018), http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

business practices to ensure that its regulatory approach is grounded in facts. While the U.S. economy has become increasingly data driven, the FTC's budget has declined an estimated five percent over the course of this decade.⁷ The FTC should be given more authority to police consumer privacy, but it cannot achieve this mission without sufficient funding or personnel.

How can regulators balance consumers' privacy goals with business innovation?

CCIA supports the GAO's recognition that regulations must be balanced with organizations' needs to provide services and to pursue socially beneficial innovation. Overly broad or prescriptive regulatory requirements would create significant overhead costs and record-keeping demands on small companies and raise the barriers to entry for new market players. Privacy legislation should, therefore, set baseline requirements, while providing industry with flexibility in meeting those requirements. Requirements should also be scalable based on context, such as organizations' scale and resources, and the sensitivity and uses of that data at issue. Finally, enforcement should account for and be proportionate to the risk of harm caused by noncompliant practices.

Federal baseline privacy legislation should be rooted in the Fair Information Practice Principles (FIPPs), which are at the heart of global privacy regimes worldwide and have proven to be flexible and durable over time. In addition to robust enforcement carried out by the FTC, appropriately balanced federal baseline privacy legislation should be characterized by extensive transparency requirements and meaningful consumer controls. Organizations should be transparent about what data they are collecting, how they are using it, and when and why data may be transferred to third parties. Consumers should also have the right to object to data processing where feasible, and to reasonably access, correct, and request the deletion of their personal information. Entrenching these rights and obligations through a baseline privacy law will allow consumers to exercise greater choice and control in the digital economy, promote competition on privacy within industry, and preserve American innovation and competitiveness.

Conclusion

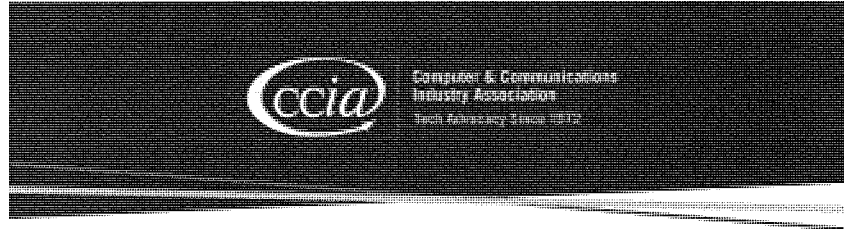
We look forward to working with you and other stakeholders on a strong and flexible modern privacy framework for the digital economy. Thank you again for holding today's important hearing.

Sincerely,



Edward J. Black
President & CEO
Computer & Communications Industry Association

⁷ John A. Howes, Jr. & Jacqueline Yin, *Comments of CCIA before NTIA on Developing the Administration's Approach to Consumer Privacy*, Computer & Comm'n's Indus. Ass'n (Nov. 7, 2018), <http://www.cciainet.org/wp-content/uploads/2018/11/CCIA-NTIA-Privacy-Comments.pdf>.



PRIVACY PRINCIPLES: A New Framework for Protecting Data and Promoting Innovation

Purpose

As the world becomes increasingly data-focused, attention has inevitably shifted to the impact of data on consumers and whether and how improvements should be made. Recent controversies have shifted how companies and consumers think about how data is collected and used online, generating some positive responses in terms of practice and transparency. It is important for the U.S. to have a healthy data ecosystem with transparency and accountability, which will help drive innovation and U.S. competitiveness.

CCIA supports the development of baseline, Federal privacy legislation that would ensure that data is handled responsibly and with transparency while also ensuring that individuals can benefit from innovation and new technologies. Such a framework should be technology-neutral, meaning it should not provide specific technology mandates; sector-neutral, meaning it should apply to online and offline organizations; and it should provide for safe harbors and flexibility for organizations to make adjustments according to the needs of individuals and evolving technology. CCIA presents these "Privacy Principles" to help guide the development of a national policy on consumer privacy.

Policy Overview

These principles aim to protect data through a robust, technology-neutral framework for assessing and managing privacy risks to individuals and organizations, and to promote innovation, in both digital services and privacy protection. Organizations across the digital ecosystem use personal data to provide innovative services. Responsible data use can be beneficial for people, businesses, and society. Reasonable data protection measures that align with individuals' expectations can protect people and communities from harms that result from misuse of data and help maintain the trust that enables the digital economy.



When evaluating the reasonability of an organization's data protection practices, it is important to understand the context in which an organization collects, processes, and uses personal information. This context can include the nature of the relationship between an individual and the organization; the potential benefits an individual, organization, and society might receive from particular uses of information; and individuals' expectations regarding data protection.

Individuals depend on organizations to use their data responsibly and be transparent about what they are collecting and how they are collecting and using it. Therefore, organizations must respect individuals' interests when they process personal information. Organizations should make reasonable best efforts to account for and mitigate potential harms to individuals, communities, and society.

Scope and Definitions

Personal information or data include any data under the control of a covered organization, that is not de-identified or otherwise generally available to the public through lawful means, and is linked or practically linkable to a specific individual, or linked to a specific device or account that is associated with or routinely used by an individual.

Different types of personal data can vary in sensitivity, depending on the context. However, some personal data is almost always sensitive. This includes data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation, and certain data of known minors.

Privacy risk

The potential for personal information, on its own or when linked to other information that might identify an individual, to cause economic loss, discrimination, exclusion, loss of self determination, or physical, reputational, or professional harm to an individual.

Covered organizations or entities include all organizations that process personal information regardless of whether they have a direct or commercial relationship with an individual whose information they hold.

Proportionality

Reasonable data protection practices may differ across covered organizations. Context, including an organization's scale and resources, the sensitivity of the data it holds, and its uses for that data, should inform the measures that it puts in place to protect data.

Interoperability

Cross-border data flows are essential to the modern economy. Organizations and individuals benefit from consistent compliance programs based on widely shared principles of data protection. These principles are intended to be interoperable and consistent with existing cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms.

Requirements for Organizations**Control**

Covered organizations must provide appropriate mechanisms for individual control, considering the service. Individuals should be able to object to data processing where it is feasible, but specific consent should not be mandatory for every aspect of data processing, which could create an overly complex and confusing experience for the individual and divert from the overall goals that the policy seeks to achieve. Policymakers should also keep in mind that the responsible processing of personal information is necessary to simply operate some services.

Access

Individuals must be able to access the personal information that they have provided to a covered organization, and it should be made available for export in a machine-readable format.

Accuracy

Personal information should be accurate, current, and complete to the extent possible for the purpose for which the covered organization maintains the data.

Deletion

Pursuant to the above "Access" principle, covered organizations should afford users with the ability to correct and/or delete the data that they provide to that organization when it would be practical and provided that deletion would not implicate the personal information of others.

Portability

Covered organizations should make reasonable efforts to enable authenticated users to obtain data they provide to that organization for their own purposes or for use with a different organization or service, provided that these data portability tools do not implicate the personal information of others. Data transfers between covered organizations should be private, secure, and balanced. Data portability tools should: (1) allow users to download and move data they have provided to the service, but not data that may relate to other users; (2) afford users control over how and when the tools are used; and (3) be tailored to the privacy and security expectations of specific products and services. Further, data portability tools should enable machine-to-machine transfers where technically feasible.

Security and Integrity

Users should expect that organizations handling their data will do so carefully and responsibly with reasonable measures to protect personal information from unauthorized access, misuse, modification, disclosure, loss, and destruction. Policy should account for and be proportionate to the risk of harm. Organizations should follow consensus best practices, and if a security breach occurs, organizations should notify individuals expeditiously when there is a significant risk of harm.

Onward Transfers

Covered organizations should ensure that personal information that they collect or process is protected in a manner consistent with the above principles even if it is transferred to third parties. Covered organizations should use enforceable mechanisms and independent audits to ensure that third parties protect data according to these principles.

Accountability**Transparency**

Covered organizations must be transparent about the types of personal information that they are collecting and how they are collecting and using it. Covered organizations should be clear about whether the personal information may be transferred to third parties, how long information may be retained, and what choices and controls individuals have with respect to their personal information. Covered organizations should make reasonable efforts to actively inform individuals, making the information relevant and actionable, about data use in the context of the relevant services.

Accountability

Covered organizations should be held accountable for meeting the requirements set out in these Privacy Principles. Covered organizations should regularly assess the privacy risks associated with their collection, processing, and use of personal information; develop systems to mitigate risks in a reasonable and proportionate manner; and monitor services for bias and disparate impacts. Organizations should practice privacy by design, building products and services that prioritize privacy, security, reliability, and reduce the likelihood of vulnerabilities, which will help earn user trust. Policymakers should set baseline requirements but enable flexibility to meet those requirements and promote industry accountability programs and safe harbors.

Enforcement

A robust federal baseline would provide clear standards for covered organizations and ensure that individuals across the United States can expect consistent data protections from organizations that retain their data. A national, privacy framework should be consistent throughout the United States, so state laws concerning data privacy, security, and breach notifications should be preempted where appropriate. This framework should be enforced primarily by the FTC at the federal level, but it should allow for enforcement by state attorneys general where the FTC has declined to act.

February 13, 2019

The Honorable Roger Wicker
Chairman
Senate Committee on Commerce,
Science, & Transportation
512 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Maria Cantwell
Ranking Member
Senate Committee on Commerce,
Science, & Transportation
425 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Lindsey Graham
Chairman
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Dianne Feinstein
Ranking Member
Senate Committee on the Judiciary
152 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Frank Pallone, Jr
Chairman
House Committee on Energy and
Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Greg Walden
Ranking Member
House Committee on Energy and
Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Jerrold Nadler
Chairman
House Committee on the Judiciary
2141 Rayburn House Office Building
Washington, DC 20515

The Honorable Doug Collins
Ranking Member
House Committee on the Judiciary
2141 Rayburn House Office Building
Washington, DC 20515

Dear Chairs Wicker, Graham, Pallone, and Nadler, and Ranking Members Cantwell,
Feinstein, Walden and Collins:

We, the undersigned members of the civil rights and racial justice community, write to ensure that civil rights retain a fundamental place in the ongoing online privacy debate, hearings, and legislation in your committees.

For over 50 years, federal law has prohibited discrimination and our economy has thrived as more people had opportunities to pursue their dreams. Our groups have been at the forefront of ensuring that civil and human rights, equity, and equal opportunity are recognized and respected as technology, society, and the economy evolve. To further

that effort, many of the undersigned organizations supported the Civil Rights Principles for the Era of Big Data in 2014.¹

In the years since 2014, our groups have continued to raise the alarm as data security and privacy abuses have disproportionately harmed marginalized communities, especially communities of color. These harmful practices include:

- Deceptive voter suppression and misinformation targeting African Americans.
- Housing discrimination and digital redlining.
- Employment discrimination through profiling and targeted advertising.
- Predatory lending, such as for student loans and payday loans.
- Exploitation of poor tech literacy through misleading notice and choice practices.
- Facilitation of discriminatory government surveillance and policing practices.

These practices violate the Civil Rights Principles for the Era of Big Data, which underscore the importance of ensuring fairness in automated decisions, enhancing individual control of personal information, and protecting people from inaccurate data.

Civil rights protections have existed in brick-and-mortar commerce for decades. It is time to ensure they apply to the internet economy as well. Platforms and other online services should not be permitted to use consumer data to discriminate against protected classes or deny them opportunities in commerce, housing, and employment, or full participation in our democracy. Companies also should be required to be transparent about their collection and use of personal information in automated decisionmaking, and to anticipate and protect against discriminatory uses and disparate impacts of big data.

To address these concerns, any new privacy legislation should be consistent with the Civil Rights Principles for the Era of Big Data:

- *Stop High-Tech Profiling.* New surveillance tools and data gathering techniques that can assemble detailed information about any person or group create a heightened risk of profiling and discrimination. Clear limitations and robust audit mechanisms are necessary to make sure that if these tools are used it is in a responsible and equitable way.
- *Ensure Fairness in Automated Decisions.* Computerized decisionmaking in areas such as employment, health, education, and lending must be judged by its impact on real people, must operate fairly for all communities, and in particular

¹ The Leadership Conference on Civil and Human Rights, *Civil Rights Principles for the Era of Big Data*, (Feb. 27, 2014), <https://civilrights.org/civil-rights-principles-era-big-data/>.

must protect the interests of those that are disadvantaged or that have historically been the subject of discrimination. Systems that are blind to the preexisting disparities faced by such communities can easily reach decisions that reinforce existing inequities. Independent review and other remedies may be necessary to assure that a system works fairly.

- *Preserve Constitutional Principles.* Search warrants and other independent oversight of law enforcement are particularly important for communities of color and for religious and ethnic minorities, who often face disproportionate scrutiny. Government databases must not be allowed to undermine core legal protections, including those of privacy and freedom of association.
- *Enhance Individual Control of Personal Information.* Personal information that is known to a corporation — such as the moment-to-moment record of a person's movements or communications — can easily be used by companies and the government against vulnerable populations, including women, the formerly incarcerated, immigrants, religious minorities, the LGBT community, and young people. Individuals should have meaningful, flexible control over how a corporation gathers data from them, and how it uses and shares that data. Non-public information should not be disclosed to the government without judicial process.
- *Protect People from Inaccurate Data.* Government and corporate databases must allow everyone — including the urban and rural poor, people with disabilities, seniors, and people who lack access to the Internet — to appropriately ensure the accuracy of personal information that is used to make important decisions about them. This requires disclosure of the underlying data, and the right to correct it when inaccurate.

Privacy rights are civil rights. Protecting privacy in the era of big data means protecting against uses of consumer information that concentrate harms on marginalized communities while concentrating profits elsewhere. Both individuals and the government must be empowered to enforce these fundamental principles of civil rights through agency rulemaking authority, strong enforcement, and the availability of effective legal redress. Historically, marginalized communities could not rely on government actors to protect their rights; this is why most civil rights laws contain a private right of action. **Privacy legislation that does not reflect these values should be rejected.**

It is long past time to see effective privacy laws for commercial data practices established in the United States. We look forward to offering our expertise and vision as the debate continues and your committees craft legislation to protect everyone's rights and create a more just and equitable society.

Sincerely,

Access Humboldt	Lawyers' Committee for Civil Rights Under
Access Now	Law
ACLU	Media Alliance
Action Center on Race and Equity (ACRE)	Media Mobilizing Project
Algorithmic Justice League	NAACP
Asian Americans Advancing Justice – AAJC	National Consumer Law Center (on behalf of its low income clients)
Campaign for a Commercial-Free Childhood	National Hispanic Media Coalition
Center for Democracy & Technology	National Organization for Women (NOW) Foundation
Center for Digital Democracy	National Urban League
Center for Media Justice	New America Public Interest Technology
Center on Privacy & Technology at Georgetown Law	New America's Open Technology Institute
Color Of Change	Open MIC (Open Media and Information Companies Initiative)
Common Cause	Organization United for Respect
Common Sense Media	Partnership for Working Families
Consumer Action	Public Citizen
Consumer Federation of America	Public Knowledge
Consumer Watchdog	Ranking Digital Rights
Electronic Privacy Information Center	Stop Online Violence Against Women
Ella Baker Center for Human Rights	The Leadership Conference on Civil and Human Rights
Fight for the Future	UnidosUS
Free Press Action	United Church of Christ, OC Inc.
Human Rights Campaign	Upturn

February 25, 2019

The Honorable Frank Pallone
Chairman
U.S. House Committee on Energy &
Commerce
2107 Rayburn House Office Bldg
Washington, DC 20515

The Honorable Greg Walden
Ranking Member
U.S. House Committee on Energy &
Commerce
2185 Rayburn House Office Bldg
Washington, DC 20515

The Honorable Jan Schakowsky
Chairwoman
U.S. House Committee on Energy &
Commerce
2367 Rayburn House Office Bldg
Washington, DC 20515

The Honorable Cathy McMorris-Rodgers
Ranking Member
U.S. House Committee on Energy &
Commerce
1035 Longworth House Office Bldg
Washington, DC 20515

RE: Main Street Associations' Support for Consumer Data Privacy Principles

Dear Chairman Pallone, Ranking Member Walden, Chairwoman Schakowsky, and Ranking Member McMorris-Rodgers;

The undersigned associations represent over a million Main Street businesses in industries that directly serve their consumers, help support communities across the country, and that Americans know and interact with every day.

Our members have no higher priority than relationships with their customers. One key aspect of those relationships is respecting the personal information that customers share with businesses. Virtually every industry sector – whether consumer-facing or business-to-business – handles significant volumes of consumer information. To comprehensively protect Americans, any federal data privacy legislation should apply to all industry sectors, and not contain any loopholes that leave consumers unprotected when their personal data is handled by a business. All of the companies involved in handling that chain of data should have legal obligations to properly guard it under privacy law, and the law should not solely rely on private contracts to create those legal obligations.

Considering that the protection of consumer data privacy is a priority issue for Congress, and should be for all businesses and consumers across the nation, below are the key principles our associations collectively support in federal privacy legislation that would establish a uniform, nationwide and consumer-centric data privacy law:

1. Industry Neutrality and Equal Protection for Consumers Across Business Sectors – Federal data privacy frameworks and legislation should apply requirements to all industries that handle personal data and not place a disproportionate burden on certain sectors of the economy while simultaneously exempting other sectors from providing equal protection of consumer data. An equivalent data privacy standard should apply, regardless of whether a business directly collected data from a consumer or obtained

it in a business-to-business transaction; federal law should provide consumer data with uniform legal protections across industries.

2. Direct Statutory Obligations for All Entities that Handle Consumer Data – Effective consumer protection regulations cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. Data service providers and other third parties need direct statutory obligations to ensure they comply with relevant laws; particularly those offering transmission, storage, analytical processing or other consumer data services for thousands of small businesses.
3. Preservation of Customer Rewards and Benefits – Any federal data privacy framework should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships and set the terms of those relationships. Federal law should include safe harbors to ensure that consumers can purchase or otherwise obtain the goods and services they want by taking advantage of the benefits, incentives or enhanced services they earn from being loyal customers, even if other customers choose not to engage in such programs. For businesses to offer such programs, they must necessarily keep track of the business transactions of their customers who choose to enroll in such programs in order to offer rewards and allocate benefits.
4. Transparency and Customer Choice – Consumers deserve to know what categories of personal data businesses collect and how that data is generally used. These policies should be clearly disclosed in company privacy policies readily accessible to consumers to ensure that they can learn how customer data is collected and used by the business to provide goods or services.
5. Accountability for Business's Own Actions - Privacy law should not include terms that could potentially expose businesses, including contractors and franchises, to liability for the actions or non-compliance of a business partner. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability if other types of businesses do not fulfill their own obligations under the law.
6. Establishing Uniform Nationwide Rules and Enforcement for Data Privacy – Congress should create a sensible, uniform federal framework for data-privacy regulation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws and enacting an alternative set of nationwide rules is necessary to achieve the important, national public policy goal of uniformity.

7. Data Security & Breach Notification – A federal data privacy law should include provisions codifying a national and reasonable data security standard for businesses, as well as a uniform process for notifying customers about data breaches. Currently, many, but not all, industry sectors are required to comply with 54 different state and U.S. territorial laws on data breach notification requirements, and nearly half of the states have enacted data security laws. All businesses should be required to protect personal data and make notice of their own breaches to affected consumers.

The principles above, which are supported by the undersigned organizations, are important to ensure that any federal legislation on data privacy protects consumers in a nationwide, uniform and consistent way. A federal law should not pick regulatory winners and losers among differing business sectors. Additionally, it should not create loopholes that leave consumers vulnerable if their data is handled by a business sector left without legal requirements or with outdated requirements.

We urge you to consider these key principles as you develop federal data privacy legislation. Additionally, we urge you to continue to solicit input from all affected industries and from businesses of all sizes during the legislative process. Otherwise, there is a risk of the federal government imposing unfair or crippling burdens on some sectors of the robust American consumer economy but not other sectors that should bear a similar responsibility for protecting the same consumer data.

We appreciate your consideration of our recommendations and we look forward to a constructive dialogue with you on these matters during the 116th Congress.

Sincerely,

American Hotel & Lodging Association
 International Franchise Association
 National Association of Convenience Stores
 National Association of Home Builders
 National Association of Realtors
 National Association of Truck Stop Operators
 National Council of Chain Restaurants
 National Grocers Association
 National Restaurant Association
 National Retail Federation
 Petroleum Marketers Association of America
 Society of Independent Gasoline Marketers of
 America

cc: Members of the U.S. House of Representatives

Consumer Technology Association

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

February 25, 2019

Chairman Frank Pallone
House Energy and Commerce Committee

Ranking Member Greg Walden
House Energy and Commerce Committee

Chair Jan Schakowsky
House Subcommittee on Consumer
Protection and Commerce

Ranking Member Cathy McMorris Rodgers
House Subcommittee on Consumer
Protection and Commerce

Dear Chairman Pallone, Ranking Member Walden, Chair Schakowsky, and Ranking Member McMorris Rodgers;

As the Committee convenes its first hearing on data privacy and begins drafting legislation, the Consumer Technology Association (CTA) asks you to take a federal approach that increases privacy protections and allows the United States to remain the world leader in innovation. CTA is the trade association representing over 2,000 American technology companies, 80% of which are small businesses. At CTA, we work to advance government policies that encourage innovation and job and business creation.

Recent changes to Europe and California's privacy laws have created an urgent need to modernize federal law and develop a framework that creates uniform national standards for consumer privacy and gives flexibility to companies to spur innovation. The lack of a federal baseline privacy law has fostered a patchwork of state-level legislation, making it difficult for companies, especially small businesses, to comply.

The U.S. approach to privacy should maintain consumers' trust while also allowing innovation that relies on the use of data collected from consumers. Policymakers should take note that the burdensome and prescriptive regimes adopted abroad impose major costs and barriers for market entry without creating commensurate benefits to privacy. They are not effective privacy frameworks.

Thanks to thoughtful and moderate regulatory approaches by the US Congress, American firms lead the world in online innovation. American platforms are now the global standard for communication, business and entertainment. To maintain our leadership, we need a data privacy structure that represents and promotes American priorities and values. Our challenge is to create consumer-centric policies that allow consumers to share their data, while gaining access to innovative services. Our collaborative goal should be to ensure any legislation propels innovation forward instead of stymying it.

As Congress deliberates privacy, we ask that you consider:

- A Uniform, Technology-Neutral National Standard: Consistent protections across technologies, companies, agencies, and state borders are the bedrock prerequisite to ensure consumer trust, continue data-driven innovation, and realize its benefits. A preemptive federal privacy law is the most effective way to achieve such consistency.

- A Risk-Based Focus on Data: Privacy legislation should focus on the type of data at issue, recognizing that sensitive data may warrant heightened protections, rather than specific technologies or industry sectors. Legal requirements and enforcement should be focused on addressing specific, concrete privacy harms to ensure that statutory obligations advance meaningful protections and do not chill use of companies' resources.
- Freedom to Innovate: Privacy legislation should provide legal clarity while maintaining the flexibility to innovate. Privacy legislation should not inhibit small businesses' ability to innovate and compete with more established companies. Red tape imposed in the name of privacy could prevent innovative companies from proving their technologies and services in the marketplace.
- Follow Time-Tested, Consensus-Based Principles: The U.S. approach should continue to rest on the principles of transparency, consumer choice, security, and heightened protections for sensitive data. Given the complexity and marketplace impacts of privacy laws, additional principles should have widespread and broad-based support.

CTA in 2015 created Guiding Principles on personal wellness data to articulate guidance to industry on how to handle data collected from wearable devices. These voluntary principles are baseline recommendations, so companies following them retain flexibility on how to implement them, accounting for each company's unique combination of products, services, and users; while increasing consumer trust. This exercise can serve as a model for the broader tech industry to work together to advance privacy principles.

- FTC Leadership: The FTC is the appropriate federal agency to enforce consumer privacy. It has generally used its authority to act against companies whose data practices caused significant harm to consumers. The FTC's case-by-case enforcement approach to privacy permits innovative uses of data but ensures that consumers are protected against harmful conduct.

We recognize the importance of consumer trust in our industry. Our members must be good stewards of the consumers' data. While there have been challenges highlighting the need for another look at managing data practices and protection, we believe a balanced approach will ensure consumer data is protected and enable businesses to grow and innovate. By working together, federal and industry leaders can develop a uniform, national framework that appropriately values consumer privacy and encourages economic growth. CTA stands ready and willing to provide our feedback as you draft and consider federal privacy legislation.

Thank you,



Gary Shapiro
President and CEO



November 9, 2018

**Comments of Engine regarding the Department of Commerce's Request for Comments on
Developing the Administration's Approach to Consumer Privacy
(Docket Number: 180821780-8780-01)**

I. Introduction

Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Engine works with government and a community of thousands of high-technology, growth-oriented startups across the nation to support the development of technology entrepreneurship. Engine promotes an environment where technological innovation and entrepreneurship can thrive by providing knowledge about the startup economy and helping to construct smarter public policy. To that end, Engine conducts research, organizes events, and spearheads campaigns to educate elected officials, the entrepreneur community, and the general public on issues vital to fostering technological innovation.

As a non-profit, Engine works with a nationwide network of startups to understand how ongoing policy debates affect new and small high-growth technology companies and how to best advocate on behalf of the ever-changing and growing startup ecosystem in the U.S. Engine appreciates the opportunity to submit comments on the Administration's proposed approach to advancing consumer privacy while protecting prosperity and innovation. The thriving U.S. startup ecosystem is responsible for some of the most innovative products and services as well as the vast majority of net job growth in the U.S.¹ Creating regulatory or legislative burdens in the name of protecting users' privacy without fully understanding the actual privacy benefits and the very real threats to startups would risk unnecessarily crippling one of the most important sectors in our economy.

II. General comments

The surge in interest around privacy protections for U.S. consumers understandably comes after several high profile missteps by some of the world's largest Internet companies. Engine appreciates

¹Kane, T. (2010). The Importance of Startups in Job Creation and Job Destruction. Retrieved from: https://www.kauffman.org/-/media/kauffman_org/research-reports-and-covers/2010/07/firm_formation_importance_of_startups.pdf



the Administration's efforts to foster a nuanced and balanced conversation around privacy that extends beyond those missteps and includes recognition of the potential impact on startups and other small businesses.

Privacy and security are top priorities for startups, which typically can't afford the reputational hit from a bombshell news report about irresponsible privacy practices as well as established Internet companies. In fact, some startups use privacy as a competitive advantage, marketing themselves to users based on the privacy protections they offer that well-known providers of similar services don't. While the trope of a young startup CEO coding an ingenious app out of a garage or dorm room with little regard for its users has pervaded popular culture, the U.S. startup ecosystem is full of companies working in good faith to protect the privacy and security of their users.

It's imperative that as the federal government looks to heighten privacy protections for U.S. consumers—especially in response to concerns prompted by the behavior of the biggest Internet companies—it not create new obligations and burdens that would be impossible for startups with bootstrap budgets and few legal resources to comply with. Creating those costly burdens would make it prohibitively difficult for new and small startups to secure enough funding and get off the ground, effectively enshrining the market power of the very companies policymakers are ostensibly concerned about.

III. Privacy outcomes

A. Transparency and accountability

Engine agrees with the Administration that consumers should be informed about how companies collect, use, store, and share their information and appreciates the Administration's acknowledgment that companies need flexibility to best provide consumers with that information depending on how a company interacts with consumers to offer a product or service. Additionally, Engine agrees that companies should conduct routine internal assessments on how they collect, use, store, and share consumer data as well as be subject to external accountability mechanisms, including regulatory bodies and privacy community watchdogs.

When discussing the obligations transferred to third-party vendors, it's worth noting how a changing regulatory landscape can uniquely impact startups and other small businesses. As the Administration states, a company that deals directly with consumers should be responsible for ensuring a certain level of accountability for privacy is carried over to the



third-party vendors who process that company's user data. Startups with small or even nonexistent legal teams lack the resources to constantly update and rewrite contracts with third-party vendors to ensure compliance with an ever-changing set of regulatory requirements.

B. Control, access, and correction

At its core, the current debate over consumer privacy online is about how much control consumers have over the data they share with companies. Engine agrees with the Administration that consumers should have reasonable control over how their data is collected, used, stored, and shared and the level of control consumers have should depend on the context in which they are sharing it, including the sensitivity of the data being shared and consumers' expectations of how it will be used. The U.S. startup ecosystem is made up of companies of all sizes across all sectors that interact with consumers in a variety of ways. Requiring intuitive controls for consumers to mandate who has access to their data and when also requires flexibility so each company can find a common-sense way to provide those controls.

Engine would like to see a federal privacy framework improve opportunities for informed user consent across the Internet ecosystem. Several policy proposals have called for either opt-in or aggressive opt-out mechanisms. Engine is concerned that either an opt-in or an aggressive opt-out regime may produce unintended negative consequences for the startup ecosystem and user privacy. Depending on how consent mechanisms are crafted, users may face "notice and consent fatigue," where the inconvenience of an ever-increasing set of privacy notifications leads consumers to blindly provide consent to avoid the hassle of processing every privacy choice. Or, if rules are crafted to make opting-out or refusing to opt-in the default choice, users may simply decline to provide consent to every data collection practice, even those that they would approve if they took the time to think about the decision. If this occurs, startups would be unable to compete in any sectors that depend on access to large datasets, because large incumbents that have been collecting user data for more than a decade would have an insurmountable advantage.

Engine also agrees that consumers should have qualified access to their own personal data held by a company and the ability, within reason, to correct or delete their own personal data that's held by a company. However, it's critical that there be clear bounds on what a user can request be corrected and deleted and that companies not be required to change or delete



data they rely on to provide their products and services, prevent fraud, or comply with legal and regulatory obligations.

IV. Goals for federal action

A. Harmonize the regulatory landscape, Interoperability, and FTC enforcement

Engine appreciates the Administration's comments on the importance of harmonizing the regulatory landscape. Since the Internet is inherently interstate and global, creating a state-by-state patchwork of laws will ensure that only companies with large legal teams are able to compete for users across state lines. A federal privacy framework should preempt individual states' privacy laws to ensure regulatory consistency and predictability, necessities for startups that are constantly launching, pivoting, and expanding.

Privacy protections should be uniform throughout the U.S., and enforcement of those protections should be predictable. Engine agrees with the Administration that the Federal Trade Commission is the federal agency most appropriate for enforcing a federal privacy framework, and Engine would support giving the FTC rulemaking authority to better enforce that framework and bring penalties for violations. Allowing other officials, including states attorneys general, to enforce a federal framework without tailored restrictions could effectively create a patchwork of 50 interpretations of a federal framework, where enforcement could dramatically vary state to state, essentially adding another layer of regulatory complexity for startups to navigate.

Engine also strongly opposes creating a private right of action, which would leave startups vulnerable to costly abusive litigation and subject them to uncertainty regarding how courts across the country will interpret obligations and penalties under a federal privacy framework. For instance, the California Consumer Privacy Act creates a private right of action for consumers whose data has been made vulnerable by a company that suffered a data breach in the absence of "reasonable" data security practices. The law also establishes statutory damages between \$100 and \$750 per user per incident and gives the courts wide discretion to determine penalties based on factors including the severity of the data breach and the company's worth. A federal framework that included that kind of private right of action—or even a broader private right of action that included any violation of a privacy law, which some have called for in California—could quickly have startups defending consumer lawsuits in several courts across the country and facing hundreds of thousands of dollars in potential



penalties. Even if such lawsuits were fundamentally meritless, the cost of litigating in multiple jurisdictions under different interpretations of the law would be ruinous for most startups.

Engine also appreciates the Administration's comments on interoperability. It's true that the Internet allows startups to grow their businesses across global borders. As other governments pursue privacy and security protections, the U.S. government should continue to champion policies that allow for the cross-border flow of data and push back on protectionist policies that would shut out competition from American startups.

B. Scalability

Engine appreciates the Administration's framing of the privacy debate as it relates to scalability, or determining the appropriateness of a regulatory burden based on "the scale and scope of the information an organization is handling" as well as distinguishing between organizations that have direct relationships with and collect data from consumers as opposed to third-party vendors that process consumer data on behalf of others. Engine agrees with the Administration that, "in general, small businesses that collect little personal information and do not maintain sensitive information about their customers should not be the primary targets of privacy-enforcement activity, so long as they make good-faith efforts to utilize privacy protections."

C. Comprehensive application

Consumers' privacy should be protected comparably across not just the Internet, but across all commercial interactions where user data is collected and stored. Since "comparable protections" does not necessarily require identical protections, the context of how a company interacts with consumers should be a major factor in how significant a burden it faces under a federal privacy framework. Engine appreciates the Administration's acknowledgment that varying business models and technologies can present different impacts on consumer privacy. Nowhere is that truer than in the startup ecosystem: an agriculture technology startup collecting temperature data should be treated differently under a federal privacy framework than an app that collects biometric information.

Outside of the type of data a company collects, the relationship between a company and consumers should be a factor when considering what kind of regulatory burdens to put on a company. In instances where consumers truly have no choice, companies should face



additional obligations and burdens. For instance, cable and telephone companies have exclusive relationships with their customers: if a customer wants to watch a television show or make a phone call, the customer's data about those actions will necessarily flow through the cable or phone company. That exclusivity is often heightened by the lack of competition in the telephone and cable markets in much of the country, often leaving customers with few choices. The Federal Communications Commission (FCC) has specific privacy rules in place recognizing the unique relationship between telephone companies and their customers. Until Congress passed a resolution under the Congressional Review Act in early 2017, there were similar privacy rules in place recognizing the unique relationship between Internet Service Providers and their customers.²

Unlike the ISP market, the Internet ecosystem is a hotbed of competition. With an open Internet, a startup with a small staff located anywhere in the country can compete with the biggest companies and reach countless users across the country and the world. While prominent companies have undoubtedly risen to the fore in certain verticals of the Internet ecosystem—such as search and social media—the Internet doesn't have several of the natural barriers to entry that the cable, telephone, and Internet service markets do. With more options to choose from online, consumers aren't forced to give their data over to any particular company and can even choose to engage with a company based on its privacy practices.

Regulators can encourage even more competition in the Internet ecosystem by boosting the industry's efforts around data portability—the policy of companies providing consumers with the means to transfer their data between competing services. Several Internet companies are already working cooperatively on the technical tools to give “all individuals across the web [the ability to] move their data between online service providers whenever

² The FCC has promulgated rules under Section 222 of the Communications Act, as added by the Telecommunications Act of 1996, to protect customer proprietary network information (CPNI), which is “personally identifiable information derived from a customer's relationship with a telephone company” and includes information such as a customer's call records. Under the law, “the general principle of confidentiality for customer information is that a carrier may only use, disclose, or permit access to customers' individually identifiable CPNI in limited circumstances: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.” Bazan, Stevens, Yeh (2007). *Government Access to Phone Calling Activity and Related Records: Legal Authorities* (CRS Report No. RL33424). Retrieved from Federation of American Scientists website: <https://fas.org/sgp/crs/intel/RL33424.pdf>



they want,”³ and the European Union’s newly implemented General Data Protection Regulation includes data portability requirements. The concept of data portability should be viewed as another way for consumers to exercise control over their data and increase competition in the Internet ecosystem, which will give startups more opportunities to challenge incumbents. While the issue will undoubtedly raise questions about which data belongs to which consumer and whether transferring one consumer’s data could pose privacy risks to another consumer, encouraging data portability will become even more critical as the debate over a federal privacy framework advances.

V. Other considerations

A. Small business exemption

The framework as laid out by the Administration doesn’t adequately consider the critical discussion around whether federal action should include an exemption for startups and other small businesses.

And while privacy advocates rightly note that even a small company can do serious privacy harms to consumers, companies covered by a small business exemption would still be subject to FTC enforcement against unfair and deceptive practices under Section 5 of the FTC Act as well as sector-specific privacy laws.

Several legislative proposals have been put forward with varying small business exceptions. Most notably, the California Consumer Privacy Act creates three criteria for determining if a company qualifies for the small business exemption. If a company has \$25 million in annual revenue, derives half or more of its annual revenue from selling personal information, or has data of 50,000 or more users, devices, or households in California, it must comply with the obligations in the law. According to the drafters, the 50,000 users, devices, or households threshold was meant to exempt the true small businesses and startups. Setting the threshold so low was misguided. A new startup that provides a service across multiple devices or collects data in the course of commonplace and frequent interactions can easily hit the threshold. For example, an app that keeps passwords for consumers is likely to be used across several devices. If that app has 13,000 users (slightly more than one quarter of the “users” a company would have before hitting the small business threshold in the California

³Data Transfer Project: <https://datatransferproject.dev/>



law) but each user has the device installed across four devices (such as two laptops, a smartphone, and a tablet), the company would serve 52,000 devices and fall outside of the law's small business exemption.

While there's no perfect answer for where to draw the line around a small business exemption, Engine supports creating a nuanced exemption based on the number of employees a company has and the company's revenue rather than on a single metric like the number of users. With the promise of the Internet, even a small company can have a user base that grows quickly and disproportionately to the actual size of the company and the ability of the company to navigate complex regulatory burdens. A legislative proposal from Reps. Suzan Delbene and Hakeem Jeffries creates a "small business exemption" that relieves companies with 500 or fewer employees from certain aspects of the proposal. Crafting a broad exemption for companies with 500 or fewer companies and a reasonable annual revenue threshold could avoid some of the anti-competitive impacts of a federal privacy regime.⁴ It's also critical that any small business exemption include an on-ramp or reasonable grace period so that companies don't suddenly find themselves in violation of privacy law. Creating a system of escalating obligations or deferred enforcement as a company meets and then surpasses the small business exemption's threshold would allow quickly growing companies to appropriately scale up their legal and compliance resources without forcing them to take on burdensome costs or risk violating the law—either of which can destroy a small, new startup—all at once.

B. Defining personal or sensitive information

Any federal action on privacy must stem from the understanding that user data fuels much of the economic growth and innovation happening online and in the U.S. startup ecosystem. But not all data is created equal, and not all data should require the same privacy protections. Startups often rely on anonymized, aggregated, or non-sensitive user data to provide, improve, and monetize their services. There is a clear consensus forming that certain types of "sensitive" or "personal" or "personally identifiable" data deserve additional protections under a federal privacy framework, including health data, financial data, precise geolocation information, and data about child users.

But several legislative proposals put forward definitions for "sensitive" or "personal" data that go far beyond the consensus around what data would actually expose consumers to

⁴ Information Transparency & Personal Data Control Act, H.R. 6864, 115th Congress (2018).



privacy harms when collected or shared. Companies regularly rely on data about how consumers use an app or navigate a website, and making it difficult or impossible to collect and share that data will only keep companies from being able to offer innovative and convenient products and services.

Equally concerning are proposals that include vague terms such as “political preferences” or “religious beliefs,” since it’s not clear if those are characteristics can be inferred from a user’s activity online. For instance, if a consumer navigates to a certain politically-leaning news website or downloads a religious text on a reading app, it’s unclear whether that would be considered data about the consumer’s political preferences or religious beliefs.

A federal privacy framework, especially one that grants the FTC rulemaking power, should include a tailored definition of “sensitive” information that triggers additional privacy protections when being collected or shared. While the FTC should have the flexibility to update its rules to keep up with changing technologies, the framework should also limit the ability the agency to dramatically alter and broaden that tailored definition of “sensitive” information.

As a part of definition sensitive or personal information, some policy proposals have put forward “non-discrimination” provisions, or language that prevents companies from offering different services or prices based on the level of data a consumer shares with the company. The California Consumer Privacy Act allows companies to offer a different service or price if a consumer exercises his rights under the law if the difference in price or service “is reasonably related to the value provided to the consumer by the consumer’s data.” Calculating the value of an individual’s data in the context of a novel startup is likely to be an impossibly ambiguous inquiry, opening the door to costly litigation over a company’s pricing decisions.⁵ For a startup that might pivot or add to existing offerings and revenue streams, it would be impossible to know the value of a consumer’s data and whether the difference in price or service could be deemed to be “reasonably related” to the difference in value to the startup between consumers who share their data and those that don’t.

⁵ In most jurisdictions, startups engaged in litigation will be unable to recover damages for lost profits because the value and likelihood of success for a new business is too speculative to properly calculate lost profits. In light of this established precedent, it seems unlikely that startups will be able to meaningfully calculate the potential lost value attributable to a single user’s data, particularly considering the value of user data is generally a function of the breadth of the data set as a whole rather than any individual data point.



VI. Conclusion

Engine appreciates the opportunity to provide feedback on the broad framework articulated in the Administration's request for comment. The outline of the discussion in the request for comment sets the table for a thoughtful and nuanced conversation around the critical issue of consumer privacy. Engine looks forward to working with the Administration and other policymakers to develop a privacy framework that protects users' privacy while encouraging innovation and promoting the thriving U.S. startup ecosystem.



Letter for the Record
February 25, 2019

House Energy and Commerce Committee
Subcommittee on Consumer Protection and Commerce
Hearing on "Protecting Consumer Privacy in the Era of Big Data"

Chairwoman Schakowsky, Ranking Member McMorris Rodgers, and members of the subcommittee:

Thank you for the opportunity to contribute to the record on the issue of consumer privacy in the era of big data. We appreciate the committee dedicating time to one of the most pressing issues facing not just the technology industry and the companies of all sizes that comprise it, but every industry and company that deals with consumer data.

Startups undoubtedly don't get the most attention in the current debate over consumer privacy, but they're the ones that stand the most to lose. With every headline-grabbing misstep by Internet giants, consumers lose trust in the Internet ecosystem. New and small startups don't have the longstanding reputations or relationships with consumers to weather those losses in trust. At the same time, as policymakers consider putting new privacy protections into law, it's the startups without large budgets and legal teams that will have the most trouble navigating a new legal and regulatory landscape. Ironically, the fear of privacy harms at the hands of Internet giants could result in rules and regulations that end up cementing the marketplace power of those very companies.

As the subcommittee continues discussing this issue, we hope lawmakers consider the perspective of the small businesses that make up the thriving U.S. startup ecosystem. As we told the National Telecommunications and Information Administration in comments last year (which are attached): "While the trope of a young startup CEO coding an ingenious app out of a garage or dorm room with little regard for its users has pervaded popular culture, the U.S. startup ecosystem is full of companies working in good faith to protect the privacy and security of their users." We hope lawmakers work to protect those companies' ability to innovate and benefit consumers while advancing privacy protections.

Sincerely,

Evan Engstrom
Executive Director
Engine

February 26, 2019

Statement for the Record

On behalf of the

American Bankers Association

before the

Consumer Protection and Commerce Subcommittee

of the

House Energy and Commerce Committee

United States House of Representatives

February 26, 2019



American
Bankers
Association

February 26, 2019

Statement for the Record
of the
American Bankers Association
for the
Consumer Protection and Commerce Subcommittee
of the
House Energy and Commerce Committee
United States House of Representatives
February 26, 2019

Chairwoman Schakowsky, Ranking Member McMorris-Rodgers, and members of the Committee, the American Bankers Association (“ABA”) appreciates the opportunity to provide its views on consumer data protection and privacy. The ABA is the voice of the nation’s \$17 trillion banking industry, which is comprised of small, midsized, regional and large banks. Together, these institutions employ more than 2 million people, safeguard \$13 trillion in deposits and extend more than \$9.5 trillion in loans. For many years, our members have had and continue to have a substantial interest in consumer data protection and privacy and we respectfully request that this statement be included as a part of the record for today’s hearing.

A. Banks and Financial Institutions Are and Have Been Subject to Extensive Privacy Laws

Banks believe strongly in protecting consumers’ sensitive personal and financial information and their privacy. For hundreds of years, customers have relied on banks to protect the privacy of their financial information. Because banks are literally at the center of people’s financial lives, our industry has long been subject to federal and state data protection and privacy laws. For example, Title V of the Gramm-Leach-Bliley Act (GLBA) not only requires banks to protect the security and confidentiality of customer records and information, but it also requires banks to provide consumers with notice of their privacy practices and limits the disclosure of financial and other consumer information with nonaffiliated third parties.

In enacting the GLBA in 1999, Congress stressed how critical privacy and data security is within the financial industry.¹ In this regard, it was Congress' intent that a financial institution's privacy practices must be readily accessible and easy to understand ("transparent") so that consumers can make well-informed choices. For example, the GLBA requires banks to provide notice to their customers about their information collection policies and practices. The notice is required to be clear and conspicuous and accurately describe the consumer's right to opt-out of the sharing of personal information with non-affiliated third parties if the bank shares customer information with such parties outside of exceptions.

Most banks make their GLBA privacy notices easily accessible on their websites. In this regard, many banks provide these disclosures using a standardized model template issued by the Consumer Financial Protection Bureau that is designed to follow the same format used for nutrition labeling on food products. The current disclosures for consumers were developed over years of effort by federal regulators and the industry. Similar transparency about data collection and information sharing that is provided by the financial sector should be available to consumers no matter the type of company with whom they do business. For purposes of Federal privacy legislation, the GLBA should be considered a tried-and-true model for transparency.

In addition to transparency, the GLBA generally prohibits a bank from providing customer information to a nonaffiliated third party unless the bank has provided the customer with notice and an opportunity to opt out and the customer has not elected to opt out of such sharing. In this regard, the GLBA contains carefully crafted exceptions to the limitations on disclosures to nonaffiliated third parties that are designed to ensure that financial markets, products and services that depend on the flow of financial information function efficiently for the benefit of the consumer, the financial institution and the financial markets generally. For example, the GLBA permits a bank to disclose customer information to a nonaffiliated third party "as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes" or in connection with "[s]ervicing or processing a financial product or service that a

¹ See 15 U.S.C. § 6801(a) (stating that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information").

February 26, 2019

consumer requests or authorizes” or “[m]aintaining or servicing the consumer’s account with” the bank. The exceptions are also designed to ensure that banks can comply with other legal and regulatory mandates and be able to share information to prevent fraud and illicit finance. Notwithstanding these exceptions, the GLBA generally prohibits a bank from disclosing a customer’s account number or similar form of access number or access code for a consumer’s credit card account, deposit account, share account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through e-mail.

The GLBA also required the federal regulatory agencies to establish standards for safeguarding customer information. These standards require financial institutions to ensure the security and confidentiality of customer information, protect against any anticipated threats to such information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. And, since April 1, 2005, the federal banking agencies have required banks to have in place incident response programs to address security incidents involving unauthorized access to customer information, including notifying customers of possible breaches when appropriate.

Banks also are subject to other, decades-old federal financial privacy and data protection laws, including the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA). The FCRA, among other things, restricts the collection, use and sharing of information that is used to determine a consumer’s eligibility for, among other things, credit, insurance or employment. The FCRA functions to limit the extent to which affiliated financial institutions may share with each other information relating to consumers, including requiring notice and an opportunity to opt out before sharing non-transaction or non-experience information (*e.g.*, application information) that is used to determine eligibility for credit. Even to the extent that the FCRA permits affiliated financial institutions to share consumer information (*e.g.*, pursuant to notice and an opportunity to opt out), the FCRA limits the use of certain information for marketing if the information is received from an affiliate, including requiring notice and an opportunity to opt out before using the information for marketing purposes.

February 26, 2019

The RFPFA protects individuals against unwarranted searches of personal financial records by the federal government. For example, a bank may not provide a federal government entity with access to copies of or the information contained in a customer's financial records except as permitted by the RFPFA (e.g., in response to a search warrant). Most states have similar laws limiting the disclosure of financial records to state government entities.

In addition, depending on their specific activities, a bank may be subject to a host of other federal privacy laws, including the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the CAN-SPAM Act, the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, and the Driver's Privacy Protection Act, among others.

Banks are also subject to strict regulatory oversight and regular exams regarding their compliance with data protection and privacy laws. This oversight includes the Federal Financial Institutions Examination Council Information Technology Examination Handbook, which is an extensive document with over 1,000 pages of IT guidance and examination instructions used by banking regulators to measure compliance with IT governance and information security program management.

In other words, the Congress has long recognized the importance of privacy for financial institutions and put into place a regulatory framework of strong privacy protections balanced with commonsense exceptions to minimize marketplace disruptions while maintaining a high level of consumer safeguards. These protections have been buttressed by a number of other laws with strong privacy protections, and banks and their federal and state regulators work aggressively to ensure consumers remain strongly protected.

We believe that it is critical that any new Federal privacy law take into consideration existing privacy laws, such as the GLBA, that apply to financial institutions and avoid provisions that duplicate or are inconsistent with those laws. Any new Federal privacy legislation should also preempt the existing patch work of state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial

system. Equally important, having a single federal standard would ensure that consumers receive the same privacy rights and protections regardless of where they may live. A variety of state laws not only makes compliance challenging for financial institutions, but makes it very difficult for consumers to understand – and protect – their own privacy rights; the greater the variation in state laws, the greater confusion and conflict between states and the less transparent the entire regime becomes.

B. State Privacy Laws

The financial services sector is concerned that if Congress does not enact uniform national privacy standards, the states will continue to attempt to fill the void with a patchwork of disparate and inconsistent requirements. In 2018, California enacted a significant new privacy law, the California Consumer Privacy Act (CCPA), prompted by a pending ballot initiative. Although an improvement over the ballot initiative, the CCPA was enacted without adequate discussion or time to fully understand the consequences. For instance, it did not take into account the many reasons data flow is important to provide consumers with the goods and services that they need or request and lacks that careful balancing that it needed. It is that balancing that is inherent in the exceptions that Congress created in GLBA.

It is important to note that the California legislature included a GLBA exception in recognition of the fact that banks and other financial institutions are already subject to Federal privacy laws and already take important steps to protect consumers' privacy rights. However, concerns remain. For example, the reach of the new law is very broad and will be subject to interpretation in implementing regulations and litigation; therefore, its full impact is uncertain. The law also includes a provision that allows consumers to request that their information be deleted, a right that could compromise law enforcement efforts to combat fraud, money laundering and terrorist financing.

Meanwhile, other states are already considering adopting privacy laws similar to, if not modeled on, the CCPA, with sufficient difference that will exacerbate the existing patch-work of different and often inconsistent state privacy and data breach laws. At this point, ten states have

introduced legislation similar to the CCPA that would provide consumers with a right to know what information is collected about them and how that information may be used. One major problem is that the definition of “consumer” and covered “personal information” is very broad and not always consistent. The CCPA defines these terms very broadly – for instance, a “consumer” can be a resident of California that is residing “for a temporary or transitory purpose” in another state. Because consumer information is not anchored within a particular state as the U.S. has a very mobile population, competing state privacy regimes are likely to provide inconsistent requirements for how that information is handled. While these laws may be well-intentioned, they hamper the free flow of data needed to provide consumers and businesses with financial products and services and process financial transactions.

C. International Privacy Laws

The financial services sector also supports an open global economy that enables trade, investment, and growth through the secure and efficient transfer of data across borders. However, measures that dictate where data is stored and how data is transferred can hinder the development of technology infrastructure and reduces our ability to serve our mobile customer base. Measures that “ring-fence” data or require data to remain in the country of origin, often referred to as data localization, ultimately damage the global competitiveness of the U.S. financial services sector and serve as non-tariff barriers to trade. These restrictions limit the efficiency of technology operations, as well as the effectiveness of security and compliance programs. It is unfortunate that the European Union (EU) has chosen to go down this path through its General Data Protection Regulation (GDPR), which has extra-territorial reach that potentially impacts the operations of U.S. banks both internationally and in certain cases, domestically. Furthermore, the lack of clarity makes it difficult to understand and challenging for compliance. And, like the CCPA, the GDPR includes a provision that lets consumers request that information be deleted, which, as noted, is a problem for law enforcement.

The broad and judicially untested language of GDPR may even have an impact on community banks in the U.S. For example, some community banks are starting to question how they can continue to serve academia, military, and non-English speaking communities without

February 26, 2019

running afoul of the GDPR in light of its claim to jurisdiction over people living in the EU and websites offered in an EU language. Existing U.S. customers living, working, or studying abroad, including U.S. college students enrolled at an EU university, academia, or U.S. service members and their families stationed overseas may subject a U.S. bank to GDPR restrictions. Similarly, a community bank in the Southwest offering online banking services in Spanish to a U.S.-based Mexican immigrant community, or a bank in the Northeast offering online banking services to dual U.S.-Portugal citizens that may live, work, retire or own property in both countries may be subject to the GDPR. As a result, the GDPR could potentially reduce the availability of banking services to underserved customers in the U.S.

On the other hand, increasing the global interoperability of privacy regimes can help to mitigate localization requirements while achieving regulatory policy goals. Regional agreements such as the Asia-Pacific Economic Cooperation (APEC) cross-border privacy rule (CBPR) enable commerce supported by the free flow of data, while preserving the national authority to develop privacy requirements that best serve their policy objectives. To date, the CBPR has had diminished utility since it is not global. The financial services sector could potentially support an expansion of CBPR if it includes European Union member states and other key trading partners to effectuate its potential. Similarly, consideration should be given to other well-established privacy principles currently being used by many in the financial sector to ensure interoperability, such as Privacy by Design (PbD), accountability, data retention and use limitations and protection of cross-border transfers of data.

CONCLUSION

The ABA shares the Committee's goal of protecting sensitive consumer personal and financial information and privacy. Banks and other financial institutions are already subject to the GLBA and other Federal financial privacy laws. We believe that it is critical that any new Federal privacy law take into consideration existing privacy laws, such as the GLBA, that apply to financial institutions and avoid provisions that duplicate or are inconsistent with those laws. Any new Federal privacy legislation should also preempt the existing patch work of state laws to

February 26, 2019

avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system and make privacy rights less transparent to consumers.



February 26, 2019

The Honorable Frank Pallone, Jr.
Chairman, Committee on Energy
and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Greg Walden
Ranking Member, Committee on Energy
and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Chairman, Subcommittee on
Consumer Protection and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member, Subcommittee on
Consumer Protection and Commerce
United States House of Representatives
Washington, DC 20515

RE: Hearing on "Protecting Consumer Data in the Era of Big Data"

Dear Chairmen Pallone and Schakowsky and Ranking Members Walden and McMorris Rodgers:

The National Retail Federation appreciates your leadership in holding today's first hearing of the 116th Congress on consumer data privacy issues. Over the past several decades, NRF has worked closely with its member companies on data privacy statutes and regulations here and abroad. Below we share some principles for U.S. privacy legislation based on the lessons learned from our work over the past three years on the General Data Protection Regulation (GDPR), which was adopted by the European Union (EU) in 2016 and took effect in 2018. Our views on federal legislation are also informed by our significant involvement over the past year on the California Consumer Privacy Act (CCPA), which was enacted last summer and will take effect in 2020.

We view our recent engagements in the GDPR and CCPA as part of a continuum of activity to help the retail industry develop best practices on data privacy and security matters since the late 1990s. Since that time, we have worked with members of this Committee and other Congressional committees on data privacy and data security legislation, and we look forward to continuing our important collaboration with you and other interested members of Congress to help develop federal privacy legislation that the retail industry could support.

NRF is the world's largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and internet retailers from the United States and more than 45 countries. Retail is the nation's largest private-sector employer, supporting one in four U.S. jobs — 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

Retailers' Use of Customer Data and Interests in Protecting Consumer Privacy

Protecting consumer privacy is one of retailers' highest priorities. Retailers know that establishing long-term relationships with their customers requires more than just providing the merchandise they want at the prices they are willing to pay. Successful retailers win their customers' trust and provide a satisfying shopping experience so that consumers continue to shop with them time and again. A critical element of establishing that trusted relationship lies in how retailers act as reliable stewards of the information their customers share with them when shopping.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations for high quality service. Whether offering goods online or in store, retailers use customer data to provide personalized experiences that consumers value. Customers, in turn, expect retailers to process their personal data responsibly and seamlessly when they are shopping. To meet these high customer expectations, retailers invest heavily in technology and spend years developing appropriate methods to comply with state, federal and global data protection regulations in ways that further their customer relationships and does not frustrate them.

In short, retailers use consumer data for the principal purpose of serving their customers as they wish to be served; retailers' data use is not an end in itself but merely a means to achieving the goal of improved customer service. This practice differentiates retailers' principal use of customer data from other businesses – typically service providers, data brokers and other third parties unknown to the consumer – whose principal business is to monetize consumer data by collecting, processing and selling it to other parties as a business-to-business service. Such data practices are the profit center of the “Big Data” industries whose products are the consumers themselves (and not goods sold to consumers). **As members of the Committee consider federal privacy legislation, it is important to recognize the fundamental differences in consumer data usage between two categories of businesses:**

- **“first-party” businesses**, which sell goods or services directly to consumers and use their data to facilitate sales, provide personalization, recommendations and customer service; and
- **“third-party” businesses**, which process and traffic in consumers' personal data, very often without their knowledge of who is handling their personal data and for what purpose.

Federal Trade Commission Views on First-Party vs. Third-Party Data Uses

In 2009, the Federal Trade Commission explained in its staff report on online behavioral advertising the distinct differences they found between first-party and third-party uses of data, particularly regarding consumers' reasonable expectations, their understanding of why they may receive certain advertising, and their ability to register concerns with, or avoid, the practice, as follows:

For example, under the “first party” model, a consumer visiting an online retailer's website may receive a recommendation for a product based upon the consumer's prior purchases or browsing activities at that site (e.g., “based on your interest in travel, you might enjoy the following books”). In such case, the tracking of the consumer's online activities in order to deliver a recommendation or advertisement tailored to the consumer's inferred interests involves a single website where the consumer has previously purchased or looked at items. Staff believes that, given the direct

relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.¹

Consumers Concerns with Significant Privacy Violations by Third-Party Businesses

Over the past eighteen months, tens of millions of Americans learned of the significant risks of harm they personally face from irresponsible data practices by third-party businesses who are unknown to them. Members of the committee need to look no further than the recent newspaper headlines with breaking news – often on the front pages of their district’s local newspaper or the nationwide newspapers – to know which privacy violations Americans care most about:

- **AT&T selling their mobile phone subscribers’ precise GPS location data, without sufficient notice or consent, to data brokers, who in turn sold the precise GPS data to “bounty hunters”** that used it to surveil mobile locations of individuals – not just once, but tens of thousands of times;
- **Cambridge Analytica using data collected on 87 million Facebook users to conduct psychographic analyses of them based on their Facebook content and selling their findings to political clients, without the consent of 99.6% of them** (as 270,000 Facebook users had consented to data collection for academic use only without also being told their consent would provide access to data on all of the other individuals in their social network who never consented); and
- **Equifax mishandling its data breach affecting over 145 million Americans, most of whom had never heard of Equifax or knew that the credit bureau held their most sensitive personal data** before its unauthorized disclosure in a breach incident.

In the three examples above, third-party data brokers, processors and service providers violated the privacy of American consumers who cared deeply about these incidents. This is why it is so highly objectionable that leading state privacy laws, such the CCPA, and Washington state’s privacy legislation, are being crafted on the inaccurate presumption that consumers’ interest in data privacy stops at the front door of a consumer-facing business. These laws fail to recognize that consumers are equally or even more concerned with what third parties do with their sensitive information behind the scenes. We do not believe legislators voting for these state privacy bills are aware of the serious deficiencies in them, and that businesses abhorred by consumers for recent

¹ *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), pp. 26-27, available at: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>

National Retail Federation
February 26, 2019
Page 4

privacy violations qualify as service providers, processors or third parties exempt from any privacy obligations (or even requirements to notify consumers of their own breaches) under the bills that state lawmakers sponsor and vote to enact. We urge this Committee to examine these flaws in state privacy laws and improve upon them by holding accountable all entities handling consumer data.

Principles for Federal Data Privacy Legislation

NRF began working with our retail company members on best practices to protect customer privacy in the late 1990s, with initial efforts focused on developing principles that promoted transparency and customer choice. Over the two decades since, NRF has participated in efforts by several Congressional committees in the House and Senate to develop federal data privacy legislation. This past fall, NRF submitted comments to the National Telecommunications and Information Administration (NTIA) on high-level goals for federal legislation, a copy of which is attached for your review. Over the years, we have also submitted comments to the Federal Trade Commission (FTC) on a range of data protection issues as the FTC explored the contours of the Commission's authority, under Section 5 of the FTC Act, to protect consumers' data privacy and ensure that businesses handling consumer data employed reasonable data security practices.

American businesses today cannot solely concentrate on federal and state data privacy regulations. Conceivably, a data regulation adopted halfway around the world may impact a U.S. business operating entirely within our national borders and employing only American workers. Retailers are not immune to the significant challenges described by global tech companies to reconcile newly adopted and conflicting data privacy laws – from the EU's GDPR to California's CCPA. They are also acutely aware of the potential for 50 different U.S. states and untold foreign governments to propose new data regulations each year that have a global reach (like the nature of the data each law intends to regulate).

These proposed regulations, even if well-meaning, may ultimately make it impossible for businesses to use data as they should to serve their customers in the many ways consumers have come to expect, largely because of the risks companies could face in the form of significant government fines or business litigation if they misjudge how best to use data responsibly to serve their customers. In the end, it may be consumers who stand to lose the most if businesses cease to take advantage of technological innovations to better serve them out of fear of tripping over a hodge-podge of potentially conflicting state, national and multi-national regulations that include very high fines for any non-compliance (and some without the ability to cure minor violations).

Retailers would like to avert a global data regulation train wreck and support a U.S. federal solution to data privacy that would apply nationwide requirements uniformly across all industry sectors handling similar customer information. As the Committee reviews proposals, we would urge you to adopt several key principles that we believe are essential to federal legislation in this area of the law:

- **Nationwide Data Privacy Regulation:** Congress should create a sensible, uniform and federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that all sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting related state laws is necessary to achieve this important, national public policy goal. Without

effective preemption of state law, Congress would simply add another data privacy regulation to what may eventually become a 50-state regulatory regime, where the U.S. laws fall within a larger, unworkable global regulatory gauntlet for businesses as state, national and multi-national laws all potentially conflict. Congress's effort to bring sensibility and certainty to data regulation is as important to the future of e-commerce as maritime law was to trans-oceanic commerce centuries ago.

- **Comprehensive Application of Equivalent Privacy Regulations to All Entities:** Federal data privacy legislation should apply to all industry sectors that handle the same or similar consumer data, and Congress should not craft rules that are specific to any subset of industry or permit exemptions that pick winners and losers among competitive industry sectors. Some industry sectors cite federal laws from last century as the basis for exemptions from a new federal privacy without supporting amendments that would bring those laws up to present-day standards for consumer privacy protection. To protect consumers comprehensively, however, a federal data privacy law must apply equivalent requirements to all industry sectors handling similar sensitive personal information.
- **Transparency and Consumer Choice:** Federal legislation should promote well-understood fair information practice principles, such as transparency and consumer choice, with respect to sensitive customer data. Businesses handling such data should be transparent about their collection and use of sensitive data and should provide consumers with meaningful choices in how such data is used. Retailers support principles like the GDPR's "legitimate interest" concept as a lawful basis for processing sensitive customer data, which properly aligns consumer expectations with business needs by balancing a business's legitimate interest in processing personal information to serve its customers with the customer's interest in protecting her data from misuse. The legitimate interest basis provides the regulatory flexibility necessary to ensure that businesses can use consumer data responsibly in ways that avoid frustrating the customer experience with incessant requests for affirmative consent where it is unnecessary for lawful processing.

We have come to these conclusions on which principles are critical to a U.S. federal data privacy law through our continuous work with member companies on both the GDPR and CCPA. There are certainly lessons to be learned from each of these laws: some areas of enlightened thinking that we support, such as the GDPR's legitimate interest basis for processing customer data, as well as areas of concern that we hope members of Congress will address as they find alternative methods to achieve the public policy ends of a federal data privacy law. We address several aspects of the GDPR and CCPA below to inform members of retailers' views on each law as the Committee considers the testimony of other stakeholders offered at today's hearing.

Lessons Learned from the GDPR

With the GDPR taking full effect less than one year ago, there are still many questions that remain about how the regulation applies to critical areas of retail business operations, such as: using customer data for improved service or promotional opportunities, managing customer information databases and loyalty programs, collecting customer consents, and honoring customer rights to erase data, port data to another business, or access their personal data held by a business.

A business does not have to be a large multi-national company to feel the regulatory impact of the GDPR. Retailers operating in the U.S. with websites, mobile apps and other digital platforms serving consumers with Internet access may face new compliance standards, increased liability for violations and more stringent enforcement. While the GDPR is aimed primarily at EU-based businesses, it also applies to companies headquartered anywhere in the world that have stores in Europe or simply target sales to Europeans through the Internet, mobile apps or other remote commerce channels. The GDPR therefore has significant implications for many U.S. retailers.

Following adoption of the GDPR nearly three years ago, NRF engaged our retail company members and those of a counterpart EU-based retail trade association, EuroCommerce, in a multi-year transatlantic effort to develop the first common global retail approach to compliance with the GDPR. This collaborative work within the U.S. and European retail sectors culminated in the *GDPR Discussion Document for the Global Retail Industry*. NRF and EuroCommerce released this discussion document last year and shared it with the data protection authorities (DPAs) in each of the current twenty-eight member nations of the EU, as well as with key EU officials in Brussels.

Although our principal purpose in developing this GDPR white paper was to provide the basis for an on-going dialogue between the global retail industry and relevant stakeholders that would facilitate retail-specific approaches to GDPR compliance and enforcement, we believe this document has considerable importance for members of the Committee as you examine lessons learned from the GDPR. In developing their compliance programs to meet the GDPR's requirements, retailers have discovered several elements of the GDPR that raise similar concerns. The GDPR discussion document takes great strides to illuminate specific areas where retailers' efforts to meet consumer expectations may be frustrated by the GDPR's approach to data regulation if DPAs' interpretations of the GDPR's provisions in the retail context are not carefully drawn.

The discussion document identified six critical areas of the GDPR that are highly relevant to the Committee's examination today, specifically: data erasure; data portability; the validity of prior consents; other legal bases for processing data, like legitimate interest; data breach notification; and automated decision-making, including profiling. We have found that well-meaning requirements in certain of these GDPR provisions may not align with existing consumer expectations, and we have strived to develop a retail approach to GDPR compliance to help minimize its unintended effects. We invite you to review this document and its discussion of areas where the intended purpose of the GDPR meets up with the reality of trying to practically implement a comprehensive global data privacy regulation in a way that will not upset customers' expectations with how they like to shop and receive personalized service from their favorite retailers.

Lessons Learned from the CCPA

In California, retailers face similar issues with the State's enacted data privacy law, but their concerns have been compounded by the fact that California spent little more than a legislative week trying to accomplish what took the EU nearly a decade to achieve with the GDPR. The underwhelming results and drafting errors throughout the law are glaringly obvious, and businesses across industry sectors are facing a regulatory regime that, if it takes effect as currently drafted, may create greater costs for California consumers than benefits.

One of the more significant concerns we raised with the authors of the CCPA is that the law's anti-discrimination clause could lead to the decline of customer loyalty programs (e.g., "club" discount cards, free merchandise, rewards, coupons, advanced release programs, exclusive experiences, etc.) offered by retailers and other businesses to California residents. The CCPA puts extraordinary pressure on these customer-favored programs by creating significant liability for businesses that provide rewards or other benefits, such as preferred service or pricing, to customers who sign up for these programs.

Under the CCPA, loyalty programs under which businesses provide preferred service or pricing to customers who opted in over customers who opt out of them are permitted only so long as the "value" of the personal information to the participating consumer used by the business is met by an equivalent value in discounts or benefits received by them. This is a legal equation fraught with such ambiguity that it invites an infinite array of "economic" opinions for state courts to weigh in potentially protracted, class action litigation. Personal data that may be "priceless" in the consumers' eyes would, if its value is defined by the consumer, never equate monetarily to a reasonable discount on a product. The potential for litigation over this most basic of retail transactions could lead some stores to shut down loyalty programs altogether as an untenable business litigation risk if they determine the potential costs of lawsuits outweigh the potential benefits to the business from providing better service and discounts to their most loyal customers.

The CCPA raises other concerns that retailers will continue to address within the California legislature over the next year before the law is expected to take effect. For example, at the 11th hour, on the final day of the California legislature's 2018 session, the CCPA was amended by "clean-up" legislation to clarify the language of the bill. However, several of the so-called improvements were refinements to the exemptions in the bill that permit businesses with highly sensitive customer information to avoid the data privacy requirements that must be borne by other businesses handling the same or even less sensitive information. In some cases, there is no corresponding federal law that would require the exempted sector from providing equivalent consumer data privacy protections. The CCPA's disparate treatment of businesses handling sensitive consumer data is one reason why Congress should move forward with comprehensive federal legislation to establish a *uniform* set of requirements nationwide that applies evenly to all industry sectors handling similar sensitive personal information.

American consumers expect all businesses handling their sensitive information to do so responsibly, regardless of when and where that data is processed. By developing a data privacy law that does not pick regulatory winners and losers with the stroke of a pen before the stroke of midnight, Congress can ensure that Americans' privacy will be protected by federal law regardless of which business is collecting, transmitting, storing or otherwise processing their sensitive personal information.

We look forward to working with the Committee to help members understand the deep flaws in the California regulation that hold the potential of significantly impacting e-commerce and exasperating consumers who could lose their preferred programs and benefits that they have come to expect. Congress would do well to avoid making the quickly-considered and problematic CCPA the model for federal legislation.

National Retail Federation
February 26, 2019
Page 8

As this Committee considers federal data privacy legislation going forward, we urge you to continue to examine the lessons learned from the GDPR and CCPA, and to avoid the flaws in these and other foreign and state data regulations while preserving the more enlightened elements of the GDPR that would advance the U.S. approach to data privacy protection. We look forward to working with you and members of the Committee on federal data privacy legislation that will provide a uniform and fair framework for consumers and businesses alike that respects and promotes consumer privacy across all industry sectors.

Sincerely,



David French
Senior Vice President
Government Relations

cc: The Honorable Nancy Pelosi
The Honorable Kevin McCarthy
Members of the House of Representatives
Committee on Energy and Commerce

Attachment



November 9, 2018

Mr. David J. Redl
 Assistant Secretary for Communications and Information
 National Telecommunications and Information Administration
 U.S. Department of Commerce
 1401 Constitution Avenue, NW
 Washington, DC 20230

Re: **NRF Comments to NTIA Request for Comments published September 26, 2018:
 “Developing the Administration’s Approach to Consumer Privacy”**
(Docket No: 180821780–8780–01; RIN 0660–XC043)

Dear Mr. Redl,

In response to the Request For Comments (RFC) published by the National Telecommunications and Information Administration (NTIA) on September 26, 2018, the National Retail Federation respectfully submits below its comments for your consideration on “Developing the Administration’s Approach to Consumer Privacy.”

The National Retail Federation (NRF) is the world’s largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and internet retailers from the United States and more than 45 countries. Retail is the nation’s largest private-sector employer, supporting one in four U.S. jobs — 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation’s economy.

I. Introduction: NRF’s Efforts to Develop Retail Principles to Protect Consumer Data Privacy

NRF has worked closely with its member companies on the development of data protection policy for more than two decades. We view our active engagement with Congress and federal departments and agencies on proposed federal privacy policy as part of a continuum of our long-term efforts to help ensure the retail industry maintains best practices on data privacy and security matters. We have worked with members of the congressional committees of jurisdiction for dozens of years to develop appropriate federal legislation on data privacy matters, specifically, and we look forward to continuing our important collaboration with the newly elected 116th Congress (2019-2020) to advance federal privacy legislation that the retail industry can fully support.

Beginning in the late 1990s, NRF formed a privacy working group with its most active member companies to develop principles for retailers on customer data privacy. Absent federal or state legislation requiring specific privacy practices, members engaged in this effort to create a set of voluntary industry privacy principles reflecting the best practices of retailers with respect to the

NATIONAL RETAIL FEDERATION
 1101 New York Avenue, NW, Suite 1200
 Washington, DC 20005
www.nrf.com

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 2

information they collected about their customers. The guiding principle was that retailers should maintain the level of data privacy they reasonably anticipate would be expected of them by the shopper in a given context.

The objectives of reasonableness and meeting customer expectations are at the heart of retailers' customer privacy practices and form the foundation of data protection regulations in the U.S. and globally. While these concepts have stood the test of time, several recent regulatory developments, including the enactment of the California Consumer Privacy Act (CCPA) and the launch of the European Union's General Data Protection Regulation (GDPR), have led to industry-wide re-examinations of current privacy principles and practices. In light of these developments, our members are also undertaking a review of NRF's privacy principles and will consider appropriate updates to guide retail industry practices with respect to customer information going forward.

As we undertake our retail sector privacy review, we value the opportunity to provide our initial views for your consideration in response to your request for comments on consumer privacy that we hope will inform future Administration policy, actions and engagement. Our comments below are divided in two parts, as follows:

- First, we provide below some important contextual information about how retail companies use consumer data to better serve their customers. Retailers' customer-centric approach to consumer data is different than third-party businesses that do not interact with consumers directly but whose revenue is based on monetizing consumer data they handle. These differences between retailers and third parties help inform our industry's approach to protecting customer data privacy as well as NRF's recommendations regarding public policy approaches. This opening discussion also sets the foundation for our comments on the Administration's proposed high-level goals for federal action on consumer privacy.
- Secondly, we provide below a set of specific comments on the "High-Level Goals for Federal Action" that NTIA enumerated in part I.B. of the RFC. We agree with you that it is an important first step for the Administration to formulate its goals for federal action to "provide the leadership needed to ensure that the United States remains at the forefront of enabling innovation with strong privacy protection," as your RFC states in its second paragraph. Once a federal policy approach is appropriately framed, the Administration will then be in position to promote within that approach – through various policy tools, including federal legislation – its desired privacy outcomes for consumers.

II. Retailers' Use of Customer Data and Interests in Protecting Consumer Privacy

Protecting customer data privacy is one of retailers' highest priorities. Retailers know that establishing long-term relationships with their customers requires more than just providing the merchandise they want at the prices they are willing to pay. Successful retailers win their customers' trust and provide a satisfying shopping experience so that consumers continue to shop with them time and again. A critical element of establishing that trusted relationship lies in how well retailers perform as stewards of the information their customers share with them when shopping.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations for service. Whether online or in store, over mobile devices or through phone orders,

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 3

retailers use data to provide personalized experiences that consumers value. Customers, in turn, expect retailers to process their personal information responsibly and seamlessly when they are shopping in their retail channel of choice. To meet these high customer expectations, retailers make significant investments in technological solutions and can spend years developing comprehensive methods to comply with state, federal and global regulations on data collection and usage that will further their customer relationships and not frustrate them.

In short, retailers use customer data for the principal purpose of serving their customers as they wish to be served; the data collection is not an *end* in itself, but merely a *means* to the end of improving customer service. This practice differentiates retailers' principal use of customer data from other businesses – typically third parties unknown to the consumer – whose principal business is to monetize consumer data by collecting, processing it and selling it to other parties as a business-to-business service. As the Administration considers the appropriate goals for federal action, and as members of the 116th Congress craft federal data privacy legislation, it is important for government policymakers to recognize the fundamental differences in data usage between businesses that are known to the consumer because they serve them directly (i.e., consumer-facing businesses) and businesses that traffic in consumers' data without their knowledge.

In 2009, the Federal Trade Commission (FTC) explained in its staff report on online behavioral advertising the distinct differences between “first-party” and “third-party” uses of data, particularly regarding consumers' reasonable expectations, their understanding of why they may receive certain advertising, and their ability to register concerns with, or avoid, the practice. Indeed, millions of Americans learned of the significant risks of harm to them personally that can flow from irresponsible data practices by third-parties who are unknown to them, as we saw in the well-publicized Cambridge Analytica and Equifax incidents during the past fourteen months. The FTC's report was noteworthy in the example in which it compared retailers' use of data to third-parties:

For example, under the “first party” model, a consumer visiting an online retailer's website may receive a recommendation for a product based upon the consumer's prior purchases or browsing activities at that site (e.g., “based on your interest in travel, you might enjoy the following books”). In such case, the tracking of the consumer's online activities in order to deliver a recommendation or advertisement tailored to the consumer's inferred interests involves a single website where the consumer has previously purchased or looked at items. Staff believes that, given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.¹

¹ *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), pp. 26-27, available at: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 4

American consumers expect all businesses handling their sensitive information to do so responsibly, regardless of when and where that data is handled. By developing a data privacy law that does not pick regulatory winners and losers among industry sectors, the Administration and the 116th Congress can work together to ensure that Americans' privacy will be protected by federal law regardless of which business is collecting, transmitting, storing or otherwise processing their sensitive personal information. We support the Administration's efforts to lead these efforts by establishing the high-level goals for federal action to protect consumer data privacy.

As Congress and the Administration consider proposed federal data privacy legislation and regulations in the coming months and years, we look forward to working with policymakers across the government to help them understand the flaws in the approaches taken by the CCPA and GDPR, and to develop a principled approach to consumer data privacy protection that meets a reasonableness standard and consumers' expectations of privacy when interacting with American businesses.

In Part III below, we provide NRF's comments for your consideration on how the Administration could drive forward such a principles-based approach to consumer data privacy protection by establishing a broad outline for the direction that federal action should take. We agree with NTIA that this may be done by establishing a set of high-level goals for the Administration to adopt, and the views we share next provide our recommendations on how the Administration can achieve these goals through its public policy efforts and support for federal privacy legislation.

III. Specific Comments on the Administration's High-Level Goals for Federal Action

We appreciate NTIA's request for feedback on the proposed high-level goals for federal action enumerated in Part B of the RFC. NRF believes establishing such goals is the most important step that the Administration can take now to lead the direction of congressional efforts to advance federal privacy legislation. We also believe that establishing the goals for federal action is a prerequisite to the Administration's ultimate goal of achieving privacy outcomes for consumers. While a range of industry sectors and companies are developing and proposing various sets of principles to achieve particular privacy outcomes, there is *greater consensus* among industry sectors and businesses at this time regarding the set of high-level goals for federal privacy legislation.

Within this context, we focus our views in this section on what retailers believe is a consensus set of goals for federal action that reflect not only the views within our own industry sector but also across many other industry sectors. These views have been informed by our conversations and meetings to date with broad-based industry trade associations and cross-sector business coalitions representing a vast array of U.S. businesses. Our comments on how to achieve these goals include a set of principles for federal privacy legislation we have recently proposed in [NRF's letter to Chairman John Thune \(R-SD\) and Ranking Member Bill Nelson \(D-FL\)](#) that supports the U.S. Senate Commerce Committee's efforts to develop federal privacy legislation that would establish nationwide privacy rules and preempt related state privacy laws. These proposed objectives for federal privacy legislation also have been informed by our two decades of experience on data privacy policy issues and, more recently, our extensive work on the GDPR and CCPA. We hope you take into consideration our views on those laws in our letter (available for your review at the link above) in addition to the goals for federal action we provide here.

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 5

To help the Administration set the broad outline for the direction that federal action should take on consumer privacy, we offer for your consideration the following comments to what the RFC describes as a “non-exhaustive and non-prioritized list of the Administration’s priorities.” *(Please note our comments below are in the same order as the goals enumerated in Part B of the RFC.)*

1. Harmonize the Regulatory Landscape

NRF strongly agrees with the Administration’s observation in the RFC that “there is a need to avoid duplicative and contradictory privacy-related obligations placed on organizations” and that “[w]e are actively witnessing the production of a patchwork of competing and contradictory baseline laws.” We also agree that “this emerging patchwork harms the American economy and fails to improve the privacy outcomes for individuals...who may not have equal protections, depending on where the user lives.”

American businesses, including retailers, recognize that they cannot solely concentrate their data privacy protection practices on compliance with U.S. federal and state data privacy regulations. Conceivably, a data regulation adopted halfway around the world – such as in the European Union (EU) – may impact a U.S. business operating entirely within our national borders and employing only American workers. Retail businesses are also acutely aware of the potential for 50 different U.S. states and an untold number of foreign governments to propose new data regulations each year that have a global reach, just like the nature of the data each law intends to regulate.

Global governmental and institutional privacy regulations, even if well-meaning in their desire to achieve privacy outcomes for consumers, may ultimately make it impossible or extremely costly for businesses to use data responsibly to serve their customers in the many ways consumers have come to expect. Moreover, proposed regulations that are not based in reasonableness and customer expectations will likely hinder the adoption and growth in innovative technology to serve customers, largely because of the risks that companies could face from government fines or penalties in class action litigation if they misjudge how best to use technology to serve their customers.

We therefore urge the Administration, as we have urged other federal entities, to set as its primary goal for federal action the establishment of a uniform and fair framework for consumers and businesses alike that respects and promotes consumer privacy. This goal would best be achieved in federal legislation that can statutorily preempt conflicting state laws in the U.S., but it will also require international solutions to harmonize the U.S. rules with those in other regions of the world. With respect to global harmonization of privacy regulations to protect consumer data, we applaud the significant and successful work of the International Trade Administration of the U.S. Department of Commerce (DOC) for its efforts to maintain and improve the EU-U.S. Privacy Shield framework and to promote greater awareness and adoption of the APEC Cross-Border Privacy Rules (CBPR) System.

Failure to achieve this primary goal of federal action – to harmonize the regulatory landscape – would largely defeat the effort to achieve a consistent set of privacy outcomes for consumers because any outcomes hoped to be achieved by federal action would be lost in a sea of conflicting state and international privacy laws. Without this harmonization of consumer privacy laws, American businesses may decrease their investment in technological innovations that would better serve customers, while protecting their privacy, out of fear of tripping over a hodge-podge of potentially

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 6

conflicting state, national and multi-national regulations that each authorize excessive fines for non-compliance.

NRF's Recommendation for U.S. Federal Privacy Legislation: The Administration asks how each goal for federal action may be achieved and, as noted above, we believe harmonization of the U.S. regulatory landscape can best be achieved through the passage by Congress of federal privacy legislation. Within this broad recommendation, however, we believe that federal privacy legislation should contain the following element that would help achieve this primary goal of federal action:

- **Federal Preemption of Related U.S. State Laws:** Congress should create a sensible, uniform and federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that all sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting related state laws is necessary to achieve this important, national public policy goal. Without effective preemption of state law, Congress would simply add another data privacy regulation to what may eventually become a 50-state regulatory regime, where the U.S. laws fall within a larger, unworkable global regulatory gauntlet for businesses as state, national and multi-national laws all potentially conflict. Congress's effort to bring sensibility and certainty to data regulation is as important to the future of e-commerce as maritime law was to trans-oceanic commerce centuries ago.

2. Legal Clarity While Maintaining the Flexibility to Innovate

The Administration proposes as another goal for federal action to "ensure that organizations have clear rules that provide for legal clarity, while enabling flexibility that allows for novel business models and technologies, as well as the means to use a variety of methods to achieve consumer-privacy outcomes." NRF agrees with this objective as a fundamental goal for federal action on consumer privacy.

U.S. businesses should have the ability to work confidently within a clear but flexible national framework for consumer privacy protections without fear of unwarranted government enforcement actions and litigation over expansive interpretations of ambiguously-worded statutes and regulations. Businesses that invest in technology to fulfill their well-intentioned and good faith efforts to serve their customers in a privacy-protected manner should have the flexibility to achieve these beneficial consumer outcomes in a variety of ways, particularly in a highly competitive industry sector like the U.S. retail industry. Balancing legal clarity, flexibility and consumer privacy is essential to preserving business competition and technological innovation that benefits consumers.

We also agree that the goal of preserving both technological innovation and consumer protection simultaneously is the hallmark of U.S. leadership on privacy issues in the international arena, and the Administration should continue to seek privacy outcomes that maximize both objectives rather than trade off one for the other. The Administration should therefore work to establish a U.S. privacy framework that permits competitive businesses to harness the power of technological innovations to minimize and prevent individual harms from the misuse of consumer data while it strives to provide the most innovative services to American consumers. Achieving this goal would truly give consumers "the best of both worlds," and we believe it is not just aspirational.

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 7

The Administration can find very good precedents to achieve this high-level goal for federal action in U.S. and international consumer protection and privacy laws that show how legal balancing tests can effectively be used to weigh business needs and consumer interests to produce beneficial outcomes for consumers.

Section 5 of the Federal Trade Commission Act, the federal law protecting American consumers from unfair or deceptive acts or practices, requires the FTC to engage in an array of legal balancing tests that take into consideration not only the government's interest in protecting consumers but also related business realities. In many aspects of its enforcement of consumer protection laws, the FTC examines the reasonableness of business practices in light of a particular business context and set of circumstances, as well as the affected consumers' expectations, awareness and ability to avoid possible harm. In this way, the FTC Act uses a flexible framework that helps the U.S. government achieve the end result that permits robust and fair competition that best serves consumers while ensuring that they are protected from unfair and deceptive acts or practices.

When it comes to international precedents for privacy regulations, the GDPR similarly adopts some legal balancing tests – although not to the same extent as the FTC Act – to achieve privacy outcomes that aim to maximize consumer protection while providing organizations with some degree of flexibility in achieving this outcome. While retailers have identified a set of concerns with implementing critical elements of the GDPR (as discussed in further detail in the [NRF letter to the U.S. Senate Commerce Committee](#)), we also recommend the Administration review the elements of the GDPR that provide flexibility to businesses in assuring consumer privacy protections.

We urge the Administration to learn the lessons of the U.S. industry's experience with these current legal precedents and work with Congress to develop and enact a new federal privacy law that will establish a clear and flexible privacy framework benefitting consumers and businesses alike. We offer one suggested element for a U.S. federal privacy law immediately below for your consideration.

NRF's Recommendation for U.S. Federal Privacy Legislation: One way the U.S. can preserve both consumer protection and technological innovation in privacy protections is to include within the legislation itself flexible regulatory concepts (e.g., legitimate interest) that are not binary in nature (e.g., opt-in vs. opt-out). We would propose including the following elements in a federal bill that can provide legal clarity while maintaining the flexibility to innovate:

- **Legitimate Interest to Process Data:** Federal privacy legislation should promote well-understood fair information practice principles, such as transparency and consumer choice, with respect to sensitive customer data. Businesses handling such data should be transparent about their collection and use of sensitive data and should provide consumers with meaningful choices in how such data is used. Retailers support principles like the GDPR's "legitimate interest" concept as a lawful basis for processing sensitive customer data, which properly aligns consumer expectations with business needs by balancing a business's legitimate interest in processing personal information (to serve its customers) with the customer's interest in protecting her data from misuse. The legitimate interest basis for data processing provides the regulatory flexibility necessary to ensure that businesses can use consumer data responsibly in ways that avoid frustrating the customer experience with incessant notifications and/or requests for consent where it is unnecessary to do so. In this way, the legitimate interest basis ensures consumer privacy protections

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 8

through a balancing test that enables businesses to proceed confidently in using technology to better serve customers while having the flexibility to achieve required privacy outcomes in a variety of ways.

3. Comprehensive Application

We strongly agree with the Administration's goal of comprehensive application of federal approaches to consumer privacy, and specifically its conclusion that "[a]ny action addressing consumer privacy should apply to all private sector organizations that collect, store, use, or share personal data in activities that are not covered by sectoral laws." We also agree that differences in business models are best addressed through application of a risk-based and outcome-based approach, which allows for "similar data practices in similar context to be treated the same rather than through a fragmented regulatory approach."

American consumers expect *all* businesses handling their sensitive personal information to do so responsibly, regardless of when and where that data is handled or by whom. Meeting consumers' privacy expectations in this respect is crucially important within our networked economy where many businesses must share consumer information to fulfill their customers' desired transactions with respect to goods or services.

For example, when a customer uses her credit card in a retail store to make a purchase, she rightfully expects that the privacy and security of the card number will be maintained by all businesses throughout the entire transaction. That is true even though the consumer may not be aware of every business (across a variety of industry sectors) that will handle her credit card number to ensure approval of the purchase, including the:

- **retail store** where the card is initially inserted or swiped in a point-of-sale terminal;
- **telecommunications carrier** (e.g., Verizon) over whose lines the card number travels;
- **payment card processor** (e.g., First Data) that routes the payment to the card network;
- **branded card network** (e.g., Visa) whose system enables the financial transaction; and
- **financial institution** (e.g., JPMorgan Chase) that issued her the credit card.

The Administration should therefore help Congress develop a federal data privacy law that treats all businesses the same when they are handling similar consumer data in a similar context, like the typical payment card transaction example above. This would ensure that the government does not craft a law that picks regulatory winners and losers among numerous businesses that all must share the same or similar consumer data to fulfill customers' wishes. To achieve this goal, we recommend that the Administration work with Congress to enact a federal law that ensures American consumers' expectations of comprehensive privacy protections will be met by all businesses handling their sensitive data, regardless of which business is collecting, transmitting, storing or otherwise processing their sensitive personal information at any given time.

As noted above, NRF has engaged in discussions with a range of industry trade associations, including the U.S. Chamber of Commerce, which share the goal of federal action ensuring a comprehensive application of privacy regulations. In its recently released privacy principles, the U.S. Chamber highlighted the importance of "industry neutrality" noting that its privacy principles "apply to all industry sectors that handle consumer data and are not specific to any subset of industry

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 9

sectors.”² NRF will continue to collaborate with the U.S. Chamber and other industry trade associations in endorsing this important goal for federal action proposed by the Administration.

In addition to the consensus position of national trade associations that support this principle, we urge the Administration to fully examine the lessons to be learned from state laws of *purported* general application which contain statutory language does not ensure consumers’ expectations of privacy will be met comprehensively across industry. As we did in the NRF letter to the U.S. Senate Commerce Committee, we have raised concerns about the CCPA, enacted by the California state legislature this past summer, and its lack of comprehensive application of its regulations to businesses handling the same or similar consumer data. On August 31, 2018, the final day of the California legislative session, the CCPA was amended by passage of “clean-up” legislation to clarify the statutory language of the law that had been enacted two months before, on June 28, 2018. However, several of the so-called improvements were refinements to the *exemptions* in the law that permit businesses with highly sensitive customer information to avoid the data privacy requirements that must be borne by other businesses handling the same or even less sensitive information.

While we agree with the intended goal of avoiding duplicative regulations at the federal and state level, which is consistent with our harmonization comments above, we highlight for the Administration that for many provisions of the CCPA, there is actually no corresponding federal privacy law that would require the exempted industry sector from providing *equivalent* consumer data privacy protections. The CCPA’s disparate treatment of businesses handling sensitive consumer data is one reason why Congress should move forward with comprehensive federal legislation that preempts the CCPA in favor of establishing a uniform set of requirements nationwide that applies evenly to all industry sectors handling similar sensitive personal information.

NRF’s Recommendation for U.S. Federal Privacy Legislation: In order to achieve the Administration’s proposed goal of comprehensive application of a federal approach to consumer privacy for all U.S. private sector organizations, we recommend that Congress craft a federal data privacy law that meets the following principle of uniform application of the law:

- **Uniform Application of Federal Law to All Entities:** Federal data privacy legislation should apply to all industry sectors that handle the same or similar consumer data, and Congress should not craft rules that are specific to any subset of industry or permit exemptions that pick winners and losers among competitive industry sectors. To protect consumers comprehensively, a federal data privacy law should apply equivalent requirements to all industry sectors handling similar sensitive personal information in a similar context.

4. Employ a Risk-Based and Outcome-Based Approach

The Administration correctly points out that compliance models for data privacy regulation often require cumbersome procedures for businesses and consumers “without necessarily achieving measurable privacy protections,” and it concludes that the federal “approach to privacy regulations should be based on risk modeling and focused on creating user-centric outcomes.” NRF agrees with

² *U.S. Chamber Privacy Principles* (released September 6, 2018), available at: <https://www.uschamber.com/press-release/us-chamber-releases-privacy-principles>

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 10

the Administration's recommended approach here, which is also consistent with retailers' customer-centric approach to data privacy discussed in detail above in Part II of our comments.

We agree that risk-based approaches allow organizations to balance business needs with consumer expectations when making decisions about protecting customer data. Retailers believe that consumers' most sensitive data deserves greater protection, for instance, than less sensitive data. A customer's shoe size, if mistakenly disclosed, is not harmful, whereas a credit card number that is obtained illegally by a hacker can be used to make fraudulent purchases on a customer's account. When businesses allocate their finite set of resources to protecting data, they use risk modeling to ensure that the greatest amount of resources are deployed to prevent data compromises that would cause the greatest risk to consumers and the business. Likewise, with respect to privacy outcomes, consumers would expect businesses to provide greater transparency and choice with respect to uses of their most sensitive data, and therefore greater resources should be allocated to consumer requests regarding the collection, use or sharing of that data compared to non-sensitive or non-personal data.

NRF's Recommendation for U.S. Federal Privacy Legislation: One way the Administration can achieve the goal of ensuring a risk-based approach to privacy outcomes is to set criteria in federal privacy legislation that defines the highest risk uses of data for which enhanced consumer privacy protections should be required. This approach should be scalable, where data practices having greater risk also have reasonably enhanced requirements to ensure the protection of consumer privacy. Such an approach would align with existing industry risk modeling practices that result in greater resource allocation to data uses that present greater risks to consumers. We therefore recommend that the Administration work with Congress to craft a federal data privacy law that adopts the following principle when establishing a risk-based approach to data privacy regulation:

- **Risk-Based Approach to Federal Privacy Regulations Should Scale Requirements by the Sensitivity of the Consumer Data (among other factors reflecting increased risk):** Federal data privacy legislation should adopt a regulatory framework with scalable protections that apply reasonably more enhanced privacy requirements to more sensitive consumer data. Data with the highest degree of sensitivity typically creates the greatest risk of consumer harm if misused or otherwise compromised. For example, consumers' Social Security Numbers or financial account numbers that are compromised, disclosed in a data breach by a bank or credit union, or otherwise used in an authorized manner could result in significant financial harm to a consumer, such as identity theft, account takeover or other financial fraud. Conversely, disclosure of a list of names and related mailing addresses in a direct mail marketing database may present very little risk of harm to consumers, as most of this information is already publicly available in online or printed phone books or directories. A risk-based approach adopted in federal privacy regulations applying comprehensively to all businesses should recognize these differences and ensure that businesses processing the most sensitive data have the greatest privacy protections in place to meet consumer expectations.

5. Interoperability (with International Privacy Laws)

The Administration accurately observes in its high-level interoperability goal that the global "internet-enabled economy depends on personal information moving seamlessly across borders," however foreign governments may approach consumer privacy differently and in ways that later

NRF Comments to NTIA re: Consumer Privacy
 November 9, 2018
 Page 11

require mechanisms to bridge the differences between international privacy regulations. While we agree with the Administration's statement that one of its objectives for federal action is to "reduce the friction placed on data flows," we caution it against developing a U.S. privacy framework that is merely "consistent with the international norms and frameworks in which the U.S. participates."

As the DOC's International Trade Administration recognizes, all international norms and frameworks are not created equally, and the U.S. should closely examine and evaluate whether an existing international framework in which it participates will ensure the consumer privacy outcomes it desires in the type of harmonized, flexible, comprehensive and risk-based approach to consumer privacy it advocates for use within the U.S. An international privacy regulation or framework whose principles are far different from ones our nation values, or is rigid and not focused on risk-based or outcome-based regulations, may not necessarily be a suitable privacy framework to which the U.S. government should ensure our laws are "consistent." Rather, we urge the Administration to lead the global community on international frameworks that embrace the objectives of promoting consumer protection and technological innovation simultaneously to ensure privacy outcomes that maximize consumer privacy and business needs alike. That should be the basis on which the Administration determines the frameworks in which it will "participate," and if it adopts that approach, then ensuring consistency makes sense.

As discussed above in our first recommendation for federal legislation that would harmonize the regulatory landscape, NRF believes the Administration should establish as its primary goal for federal action to work with Congress to enact a sensible, uniform and federal framework for U.S. data privacy regulation that benefits consumers and businesses alike by ensuring that all sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. We observed above that Congress's effort to bring certainty to data regulation on a global scale is equally as important to the future of e-commerce as maritime law was to trans-oceanic commerce centuries ago. Given its mission, history and institutional experience, the DOC is uniquely positioned among U.S. federal government departments to recognize the parallels drawn here and the importance of participating in international legal frameworks – consistent with U.S. principles and laws protecting consumer privacy – that enable global commerce.

In addition to the International Trade Administration's focus on international frameworks, the NTIA is fully equipped to lead the federal government's efforts to help Congress achieve the goal of enacting a uniform set of U.S. federal privacy regulations with consistent, nationwide application. After establishing a U.S. national framework – harmonization within the American legal system itself – the DOC will have greater leverage to work with its international counterparts to harmonize the new U.S. data privacy law with the laws of other nations and multi-national regions, such as the EU.

The EU recognized the same need a decade ago when it initiated its efforts to develop the GDPR with the primary goal of establishing a uniform set of data privacy rules that would apply evenly throughout its member states – twenty-eight nations of Europe. Congress now needs to do the same by passing preemptive federal data privacy legislation to give U.S. government officials the single-most important tool they need to harmonize U.S. data privacy law with international privacy laws. A comprehensive U.S. federal privacy law ensuring consumer privacy outcomes is one the DOC could support and promote worldwide as the leading global standard for data privacy regulation that protects consumer privacy without sacrificing technological innovation or business competitiveness.

6. FTC Enforcement

The Administration's high-level goal in support of the FTC as "the appropriate federal agency to enforce consumer privacy with certain exceptions made for sectoral laws outside the FTC's jurisdiction" must be carefully considered with respect to the exceptions. We agree that other federal enforcement agencies (or even certain state enforcement authorities for some industry sectors) may be required to enforce comprehensive federal regulations with the same power and authority as the FTC would enforce them against entities subject to its own jurisdiction.

The exceptions to FTC enforcement should therefore not permit *inequivalent* enforcement among federal agencies such that some may not enforce a comprehensive privacy law to the same degree against businesses within their own jurisdiction as the FTC does against businesses under its jurisdiction that are handling the same or similar sensitive data within a similar context. To address this concern, the Administration should look to enforcement harmonization models in existing federal laws that either require memorandums of understanding or inter-agency policy agreements among federal enforcement agencies to ensure that each agency with the appropriate authority enforces a comprehensive law equally against all businesses subject to its jurisdiction. Failure to adopt a similar harmonized approach to privacy law enforcement among federal agencies could create disparate treatment and even disincentives within the less-regulated industry sectors to fully assure the same customer privacy outcomes that sectors subject to FTC enforcement would ensure.

Additionally, with respect to the FTC's enforcement authority itself, the Administration should recognize that businesses subject to its jurisdiction are remarkably diverse in their size and scope of operations, and differ greatly with respect to their use of consumer data and the sensitivity of data they process. The FTC therefore employs legal balancing tests, as discussed above regarding flexible approaches, to calibrate the reasonableness of a business practice. For these reasons, "one-size-fits-all" data security standards are unworkable, and the application of one sector's data security standards to *all* commercial businesses under the FTC's jurisdiction is unwarranted, especially considering its enforcement of a *reasonable* data security standard under Section 5 of the FTC Act.

We appreciate the FTC's past recognition of the significant differences between financial institutions and retail businesses in the sensitivity of customer data they collect and use, as well as the Commission's consumer-centric and risk-based approach to enforcement of Section 5 of the FTC Act. We also appreciate the Commission's understanding of the differences in the enforcement of data security standards by the respective federal agencies for financial institutions versus commercial businesses. NRF believes the recognition of these differences by the FTC supports the position that comprehensive federal privacy legislation that includes a provision on data security for all businesses, and empowers the FTC to enforce this standard, should be reasonable and appropriate for the types of businesses to which the standards would apply.

FTC enforcement of comprehensive privacy regulations that uses a scalable reasonableness approach, grounded in determining the appropriateness of business practices in light of consumer expectations of privacy and data security, would provide the vast array of businesses subject to the FTC's jurisdiction with the necessary flexibility in their implementation of reasonable privacy and data security standards, and would permit the Commission to enforce such regulations fairly and equitably to ensure businesses' compliance with them.

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 13

7. Scalability

While NRF generally supports the high-level goal of scalability “to ensure that the proverbial sticks are used to incentivize strong consumer privacy outcomes are deployed in proportion to the scale and scope of the information an organization is handling,” we call out for comment NTIA’s statement in this section that “there should be a distinction between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations.”

As discussed in greater detail above in our support for the high-level goal of comprehensive application of the law, we describe a typical credit card transaction in which credit card numbers pass through multiple “third-party” vendors in order to complete a payment card transaction. Between the retail store, where the card is swiped, and the cardholder’s bank, which issued the card, there are many third parties that should be held to the same standards to protect the privacy of the cardholder’s sensitive personal information to the same degree as the bank that issued the card and the merchant that accepted it for payment.

The Administration’s proposal to exempt third-party vendors that process personal data on behalf of other organizations is inconsistent with its own high-level goal for comprehensive application of federal privacy regulations. We urge the Administration to consider the consumer harms that could arise if third-party vendors do not protect consumer information to the same degree as other businesses, particularly in our networked, internet-enabled and data-sharing economy.

The Administration should recall that in Part II of our comments above, we provided an overview of the context in which retailers operate and their focus on a customer-centric approach to data privacy. We also point out that the FTC considered situations in which third-parties unknown to consumers handle their personal data, and concluded that those contexts raise greater privacy concerns than ones in which first-parties (i.e., consumer-facing companies) handle the same data.

For these reasons, the Administration should reject this proposed third-party exception in its scalability goal for federal action as inconsistent with the high-level goal of comprehensive application of a federal privacy law. It is a proposed exemption that we believe, if adopted, will fail to ensure the privacy outcomes for consumers that is the purpose of the Administration’s proposed consumer-centric approach to privacy.

Wherever consumer data flows, appropriate privacy protections should follow. That is the golden principle upon which the Administration’s comprehensive application and scalability goals should rest; exemptions for third-party vendors are inconsistent with this principle.

IV. Conclusion

We have developed our views above on which principles are critical to a U.S. federal data privacy law through the past two decades of working with our member companies on data privacy policy. There are certainly lessons to be learned from recently enacted laws: some areas of enlightened thinking that we support, such as the GDPR’s legitimate interest basis for processing customer data, as well as areas of concern with the CCPA we hope the Administration addresses with Congress to find alternative methods to achieve the public policy ends of a federal data privacy law.

NRF Comments to NTIA re: Consumer Privacy
November 9, 2018
Page 14

We look forward to discussing our comments with you as the Administration develops its approach to consumer privacy and high-level goals for federal action. If you have any questions regarding our comments above, please contact Paul Martino, Vice President, Senior Policy Counsel, at MartinoP@nrf.com.

Thank you again for the opportunity to provide our views for your consideration.

Sincerely,



David French
Senior Vice President
Government Relations

cc: The Honorable John Thune
The Honorable Bill Nelson
The Honorable Greg Walden
The Honorable Frank Pallone



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electron.org

February 26, 2019

The Honorable Janice Schakowsky
Chair
Subcommittee on Consumer Protection
and Commerce
House of Representatives
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection
and Commerce
House of Representatives
Washington, DC 20515

Dear Chair Schakowsky, Ranking Member McMorris Rodgers, and Members of the Subcommittee:

The Electronic Transactions Association ("ETA") appreciates the opportunity to submit this statement for the record for the Subcommittee's hearing, "Protecting Consumer Privacy in the Era of Big Data."

ETA is the leading trade association for the payments industry, representing over 500 payments and FinTech companies that offer electronic transaction processing products and services and commercial loans, primarily to small businesses. During 2018 in North America alone, ETA members processed over \$7 trillion in consumer purchases. ETA's members include financial institutions, payment processors, FinTechs, and all other parts of the payments ecosystem.

ETA and its members support U.S. and international efforts to strengthen privacy laws in ways that help industry combat fraud and help consumers understand how their data is being used. As lawmakers and regulators explore additional ways to protect consumers, it is critical that government coordinate with the payments industry to combat fraud and cybercrime so that all consumers have access to safe, convenient, and affordable payment options and other financial services.

ETA understands the importance of protecting consumers, networks and data. ETA members have a long history of developing innovative solutions to ensure privacy and security in transactions and payments. The United States should adopt a national privacy law that protects consumers by expanding their current rights without discouraging competitiveness and innovation.

From the technology perspective, ETA's members are constantly developing and deploying new technology and tools to detect, deter, and eliminate fraud. Just a few examples of these efforts include the following:

- **Data Encryption.** The payments industry has introduced point-to-point encryption (P2PE) and the tokenization of data to minimize or eliminate the exposure of unencrypted data in connection with a purchase.
- **Improved Authentication.** The use of new authentication methods to verify and authenticate transactions helps minimize potentially fraudulent transactions. These new tools include the use of the following types of advanced tools:



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

- biometric authentication, including the use of thumbprints, facial, and voice recognition
- geolocation that compares the merchant's location with the location of the consumers phone
- behavioral biometrics (e.g., monitoring keystrokes)
- **Fraud Scoring / Suspicious Activity Monitoring.** The payments industry continues to refine tools for monitoring and analyzing payment data for suspicious activity. With improvements in machine learning and artificial intelligence, payments companies are gaining additional tools for identifying suspicious patterns in transaction data.
- **Chip Cards and EMV.** The payments industry has worked to replace magnetic stripes for credit and debit cards with a computer chip card, also called EMV. Chip cards make our payments system stronger by protecting against theft, counterfeit cards, and unauthorized use of cards in a store.

These are just some of the tools that the payments industry has developed in recent years to fight fraud, protect consumers, and ensure the integrity of the payments ecosystem. These efforts have been remarkably successful in reducing fraud while ensuring that consumers have access to fast, reliable, and safe payment options.

A robust financial system is integral to the economy because it enables the fundamental functions of economic activity, including connecting borrowers with savers, facilitating investments, processing payments, and the safekeeping of financial assets. For the U.S. financial system to remain competitive in the global economy, the United States must continue to prioritize consumer protection, safety, and reliability, while also continuing to lead in innovation.

ETA looks forward to encouraging a collaborative approach and believes a national framework should include the following principles:

- **Data Security and Breach Notification.** Congress should include risk-based data security and breach notification provisions that protect sensitive personal information pertaining to individuals. Consumers have the right to be notified within a reasonable timeframe if they have been subjected to a personal data breach. ETA understands security is different for individual businesses and a uniform national data breach framework should permit flexibility in implementing reasonable technical and physical security practices.
- **National Standard.** By providing consumers and businesses with consistent protections through an established national standard for breach notification preemptive of state laws, consumers and businesses will benefit. Enacting a federal preemption will provide certainty and consistency to businesses and consumers alike without having to navigate the patchwork of state laws. A federal preemption would also reduce the complexity and costs associated with the compliance and enforcement issues resulting from different laws.



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

- **Maximize Transparency.** Businesses must promote transparency with their customers and transparency is also important when engaging with regulators or other appropriate authorities. Regulators and government officials should be appropriately transparent about their objectives.

With respect to personal data, consumers should have reasonable access to clear and understandable statements about businesses practices and policies. Businesses should be transparent about: the types of personal data collected, how the personal data will be used, and if personal data may be disclosed and/or shared. Businesses should also provide clear privacy notices to consumers and provide appropriate procedures for individual control, including the opportunity to control data sharing.

- **Access to Data.** Individuals must have a reasonable right access their personal information that they have provided to a company, and where practical, have that information corrected. Individuals should also have the ability to request the deletion of personally identifiable information provided to companies, unless there is a legitimate or legal obligation to maintain that information.
- **Permissible Uses.** The payment industry has a long commitment and history of fighting fraud. The industry is constantly developing and deploying new technology to detect, deter, and eliminate fraud. New and enhanced technologies have amplified the payments industry's ability to offer new fraud solutions and strengthen our on-going efforts. Any privacy or data protection standard should include provisions for permissible uses of data to prevent fraud and protect consumers.
- **Enforcement.** To protect consumer rights and provide responsibility, enforcement needs to be consistent and coordinate between the federal government and the state's regulatory body. Congress should encourage collaboration between the appropriate federal agency and state attorney generals to enforce a national consumer privacy law. Strict coordination between the federal agency and state regulatory body should be followed to avoid duplicate or conflicting enforcement actions. Fines and other enforcements actions should be based on the harm directly caused. Other criteria that should be considered but not limited to include: the severity of the data breach, any actions taken by the business to avoid and alleviate the harm, if any negligence was found, and any negative previous history conduct involving business and personal data. However, a federal privacy law should not provide a private right of action for privacy enforcement.
- **Maintaining Flexibility.** Technology that is involved in data processing evolves rapidly. A baseline law can provide clarity on achieving specific privacy principles, however, laws and regulations should undergo reviews and be flexible. A government should not mandate a specific technological solution or other instrument to implement consumer protections. Including a safe harbor within a federal privacy law would promote the development of adaptable, consumer-friendly privacy programs.
- **Industry and Sector Neutrality.** A national privacy framework should be applied to all industry sectors that handle consumer data and such protections should be consistent for companies across products and services. It should also be technology neutral and allow



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

organizations to adopt privacy protections that are appropriate to specific risks. Protections shouldn't interfere with innovation and economic competitiveness in an evolving technology landscape.

- **Global Leadership.** Congress should adopt policies that facilitate international electronic commerce and promote consumer privacy – all which benefit, consumers, economic growth, and trade. Burdensome international regulations hamper the growth of new businesses and creates conflict of law between jurisdictions. Businesses shouldn't have to worry about foreign regulators because a few people from another country navigate to their website or use their service. Having the United States establish a national privacy framework will facilitate an international data framework and reinforce U.S. leadership worldwide.

The payments industry never rests - working tirelessly to fight fraud and protect consumers, including by developing new tools to prevent or identify fraud through the analyzing data and frequently introducing new fraud fighting solutions. Privacy laws should continue to recognize these goals and the important role the payments industry plays in combatting fraud. By working together, lawmakers, regulators, and industry can protect consumers while providing them with access to the safest and most convenient payments system in the world.

ETA would like to thank the subcommittee for this opportunity to provide this statement for the record on this important topic. We appreciate your leadership on this important issue. If you have any questions, please feel free to contact me directly at stalbott@electran.org.

Sincerely,



Scott Talbott
Senior Vice President of Government Affairs
Electronic Transactions Association

February 26, 2019

The Honorable Frank Pallone, Jr.
Chairman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Greg Walden
Ranking Member
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Chairwoman
House Committee on Energy and Commerce
Subcommittee on Consumer Protection and
Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
House Committee on Energy and Commerce
Subcommittee on Consumer Protection and
Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Pallone, Ranking Member Walden, Chairwoman Schakowsky, and Ranking Member McMorris Rodgers:

Thank you for conducting today's hearing on consumer privacy. 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, the 21st Century Privacy Coalition ("Coalition") supports federal legislation that provides stronger and more meaningful privacy protections for American consumers.¹

How Congress Can Best Protect Consumers

The Coalition strongly believes that Congress should 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 requires an opt-in consent regime for the use and sharing of customers' sensitive personally identifiable information consistent with the framework articulated by the Federal Trade Commission ("FTC") in its landmark Privacy Report.²

¹ The 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.

² See 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>.

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 a federal privacy law 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%) want the same privacy protections to apply to their personal information *regardless* of the entity that collects such information; and (2) overwhelmingly (83%) 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.³

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—as well as the context in which it is collected. For example, consumers expect sensitive information about their medical histories, financial information, 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.

The Need For a National Framework

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.

Nonetheless, preempting state laws should not mean weakening protections for consumers. A federal consumer privacy law needs to be a strong one. Congress should be able

³ See 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% of consumers favor such a consistent and technology-neutral privacy regime, and 83% 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.').

to develop a law that guarantees strong privacy rights to consumers in—and adopts the best practices from—every state.

Conclusion

The FTC should have the primary authority to enforce a national privacy law, although state attorneys general should also have authority to enforce the law. To support the agency in its mission, Congress should provide the FTC with the ability to impose civil penalties on violators for first offenses of well-defined requirements. And the Coalition strongly supports Congress providing the agency with additional resources necessary to undertake appropriate enforcement actions to keep all companies honest and compliant.

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 state privacy requirements would eliminate the consumer confusion and frustration, business 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. The Coalition looks forward to working with you and your colleagues to develop such a law.

Sincerely,

/s/ Jon Leibowitz

Co-Chair
21st Century Privacy Coalition



February 26, 2019

The Honorable Janice Schakowsky
Chairwoman
Energy and Commerce Committee
Subcommittee on Consumer Protection and
Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Energy and Commerce Committee
Subcommittee on Consumer Protection and
Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairwoman Schakowsky and Ranking Member Rodgers:

On behalf of ACA International, I am writing in regards to your hearing entitled, "Protecting Consumer Privacy in the Era of Big Data." ACA International is the leading trade association for credit and collection professionals representing approximately 3,000 members, including credit grantors, third-party collection agencies, asset buyers, attorneys, and vendor affiliates in an industry that employs more than 230,000 employees worldwide.

Without an effective collection process, the economic viability of businesses and, by extension, the American economy in general, is threatened. Recovering rightfully-owed consumer debt enables organizations to survive, helps prevent job losses, keeps credit, goods, and services available, and reduces the need for tax increases to cover governmental budget shortfalls. Furthermore, without the information that ACA members provide to consumers, they cannot make informed decisions that help preserve their ability to access credit, medical care, and a host of other goods and services. ACA members play a key role in helping consumers fulfill their financial goals and responsibilities while facilitating broad access to the credit market.

ACA appreciates that the Subcommittee is exploring ways to develop a federal data privacy standard to protect consumers. We strongly support the goal of protecting the privacy of consumers and their data. However, there are many lawful and important reasons why those in the accounts receivable management industry may collect and store consumer data. As it moves forward, it is critical that Congress is diligent in ensuring legitimate businesses are not faced with insurmountable regulatory burdens surrounding data privacy laws, particularly if they stifle innovation.

The current landscape in this area is robust including sweeping and complex state legislation such as the California Consumer Privacy Act of 2018, which also touches many businesses outside of California. Additionally, there are multiple federal laws ACA members are already complying with in this area including the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, the Gramm Leach

ASSOCIATION HEADQUARTERS
4049 WEST 70TH STREET 55435
P.O. BOX 590106, MINNEAPOLIS, MN 55449-0106
TEL (952) 926-6347 FAX (952) 926-1624

FEDERAL GOVERNMENT AFFAIRS OFFICE
309 2ND STREET NE, WASHINGTON, D.C. 20002
TEL (202) 547-2670
FAX (202) 547-2671

ACA@ACAINTERNATIONAL.ORG WWW.ACAINTERNATIONAL.ORG

Bliley Act, and the Family Educational Rights and Privacy Act of 1974. Furthermore, the General Data Protection Regulation went into effect in the European Union in May 2018 and impacts certain ACA members in the United States, as well as international accounts receivable management agencies.

As Congress moves forward with any potential new laws for federal data privacy, we ask that it is cautious not to create any duplicative, conflicting, or overly complex standards for those in the accounts receivable management industry who already work carefully to protect consumer data. Lastly, we strongly urge Congress that any law going forward should preempt state requirements in this area, so that all Americans receive the same level of privacy protections.

Thank you for your leadership in holding today's hearing. We look forward to continuing our engagement with the House Energy and Commerce Committee.

Sincerely,



Mark Neeb
Chief Executive Officer

Monday February 25, 2019

Will Rinehart
Director of Technology and Innovation Policy
American Action Forum
1747 Pennsylvania Ave
Washington, D.C. 20006

The Honorable Janice D. Schakowsky
Chair
2367 Rayburn House Office Building
Washington, DC 20515

And

The Honorable Cathy McMorris Rodgers
1035 Longworth House Office Building
Washington, D.C. 20515

Dear Chair Schakowsky and Ranking Member McMorris Rodgers,

As Congress considers privacy legislation, avoiding the imposition of excessive costs should be an important consideration. Indeed, the European General Data Protection Regulation (GDPR) serves as a warning in this regard, since it has been shown to impose substantial costs in three ways.

First, the regulation forces firms to retool data processes to realign with the new demands. This is generally a one-time fixed cost that raises the cost of all information-using entities. A McDermott-Ponemon survey on GDPR preparedness found that almost two-thirds of all companies say the regulation will "significantly change" their informational workflows.¹

Second, the regime introduces new risk, causing companies to staff up to ensure compliance. The International Association of Privacy Professionals (IAPP) estimated the regulation will cost Fortune 500 companies around \$7.8 billion to get up to speed with the law. And these won't be one-time costs since, "Global 500 companies will be hiring on average five full-time privacy employees and filling five other roles with staff members handling compliance rules."²

Finally, the law will surely change the dynamics of the industry, as companies adapt to the new requirements. For example, when the EU adopted the e-Privacy Directive in 2002, research found that venture capital investment in online news, online advertising, and cloud computing dropped by between 58 to 75 percent.³

The GDPR's effect in Europe is a cautionary tale that Congress should avoid heavy and intrusive regulation in favor of a robust but less burdensome approach to federal privacy legislation. To help,

¹ <https://iapp.org/news/a/new-study-highlights-lack-of-gdpr-preparedness/>

² <https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/>

³ <https://www.ceps.eu/sites/default/files/E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments%20in%20the%20EU.PDF>

our comments submitted to the National Telecommunications and Information Administration have been attached.

Respectfully,

Will Rinehart

Comments on Developing the Administration's Approach to Consumer Privacy
 NTIA Docket No. 180821780-8780-01
 By Will Rinehart⁴

Executive Summary

Among the most controversial parts of the European General Data Protection Regulation (GDPR) is the shift of the entire Internet ecosystem toward an opt-in system where users have to say yes to every instance of data collection. Yet, the requirement that all data collectors abide by an opt-in mandate has been gaining support among policymakers and advocates here in the United States. As talks over a comprehensive federal privacy law have become more serious, policymakers should be aware of several facts:

- Privacy is a multifaceted term, and yet, consumers tend to be more concerned about fraudulent activity such as identity theft rather than control over data;
- Advocates frame opt-in mandates as fundamental for consumer choice, yet changing a privacy regime to opt-in doesn't change the choices available to a consumer;
- Evidence suggests that users of online platforms are aware of their privacy settings and take steps to secure their data; and finally
- Privacy laws impose large costs on innovation and the online information ecosystem.

Introduction, or When to Regulate

At the very core, opt-in mandates are meant to solve an informational market failure, proponents contend.⁵ That failure occurs because consumers' choices are biased, as they aren't aware of the risks involved in disclosing information. In this sense, an informational market failure is similar to a typical market failure in that there exists, in principle, a trade that could occur between market participants that would make at least one participant better off. Yet, that trade does not occur.

The informational market failure is the first part of a three-part test that should be used for all new regulations:⁶

1. First, prove the existence of market abuse or failure by documenting actual consumer harm;
2. Then, explain how current law or rules are inadequate, and show that no alternatives exist including market correctives, deregulatory efforts, or public/private partnerships to solve the market failure; and finally
3. Demonstrate how the benefits of regulation will outweigh the potential countervailing benefits, implementation costs, and other associated regulatory burdens.

Is there a market failure in privacy? The case is thin. As will be detailed below, some make the strong claim that bias in privacy decision-making necessitates strong regulatory correctives. But the reality is far more complex. As two economists noted, "identifying an inconsistency in someone's behavioral preferences (meaning those that actually determine choice) is not the same

⁴ Will Rinehart is Director of Technology and Innovation Policy at the American Action Forum.

⁵ Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy,"

https://www.ftc.gov/system/files/documents/public_comments/2017/10/00006-141501.pdf

⁶ <https://www.americanactionforum.org/comments-for-record/policies-will-foster-growth-artificial-intelligence/>

as identifying someone's true preferences."⁷

Additionally, opt-in mandates and privacy laws place a heavy burden on innovation, and this impact is not just felt in the tech sector, but across all industries and firms that use data processing—which is increasingly all actors.

The follow comments are broken into two sections, which correspond to the first and the third parts of the test. The first part explores the problem of an information market failure that opt-in mandates are meant to correct. As should be apparent by the end, opt-in mandates do little to correct this problem, if it is indeed a problem that should be corrected. The second section reviews the literature on the cost of privacy regulations and concludes that they are onerous. Just because privacy is an important value doesn't mean privacy regulations should get a pass. Policy makers should be keenly aware of the pitfalls of privacy regulations.

Part One – The Informational Market Failure

Defining Privacy and Privacy Risk

As countless surveys attest, Internet users are concerned about and value their privacy.^{8,9,10} But privacy is a multifaceted term that can carry a variety of definitions.¹¹ Famously, Warren and Brandeis described privacy in the 1890s as the right to be left alone. Alan Westin thought privacy could be understood as the control over and safeguard of personal information, while more recent interpretations of the idea see it as an aspect of dignity, autonomy, and human freedom. For the purposes of privacy regulation, it is important to broadly distinguish data security concerns from concerns about control of data collection and use because the term privacy is often used for both.

In one sense, privacy often just means data security, the protection of digital data from the unwanted actions of unauthorized users, such as a cyberattack, a data breach, or fraud. On the other hand, privacy as term has also come to reference laws and regulations that limiting legitimate actors from using, disclosing, or collecting information. The distinction becomes especially clear when privacy as an issue of data control is explicitly broken out from data fraud, like the Census has done. Since 1994, the Census working in conjunction with the National Telecommunications and Information Administration have surveyed Internet users. When users were asked about their top concerns in the most recent polling, identity theft and credit card or banking fraud top the list, at 57

⁷ Mario J. Rizzo and Douglas Glen Whitman, "The Knowledge Problem of New Paternalism," <https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2461&context=lawreview>

⁸ Mary Madden and Lee Rainie, "Americans' Views About Data Collection and Security," <http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/#few-feel-they-have-a-lot-of-control-over-how-much-information-is-collected-about-them-in-daily-life>

⁹ Julie Beck, "People Are Changing the Way They Use Social Media," <https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/>

¹⁰ Rimma Kats, "Many Facebook Users Are Sharing Less Content," <https://www.emarketer.com/content/many-facebook-users-are-sharing-less-content-because-of-privacy-concerns>

¹¹ Adam Moore, "Defining Privacy," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1980849

percent and 45 percent.¹² Yet, concerns about data collection and loss of control over personal data rank far lower, at 22 percent and 21 percent. American Action Forum survey data confirms this finding. When the concept of privacy is broken into constituent parts, fraudulent activity is leaps and bounds more of a concern than control of data, by nearly three times.¹³

The distinction between these two versions of privacy comes in expectations. Most expect that health, banking, and financial information won't be leaked because it could affect the availability or price of employment, credit, or insurance, or it could contribute to risks of identity theft or fraud. As Joseph Farrell, formerly of the Federal Trade Commission pointed out, harms from "the unexpected revelation of previously private information" is a driving concern for consumers. Any successful policy discussion over privacy will need to carefully disaggregate these instrumental concerns from more intangible concerns like data control.¹⁴

Just as privacy is a polysemous term, so is value. Value can be understood in one context as quality of a good that makes it desirable, which is usually reflected in the price of an item. But value can also be about the propriety of an object or activity, "whether the object or activity is compatible with or supports the moral standards of the relevant individual or group."¹⁵ Thus, when discussing value of privacy, the issue of economic cost is naturally associated with larger societal values about privacy. Viewed from this lens, whether or not privacy laws actually grant consumers a higher level of protection isn't important. What is important is that pass privacy laws are passed to signaling that the United States collectively values privacy. However, just because privacy regulations are salient, that doesn't mean they are prudent.

Making the Case for Opt-in

Privacy law in the United States is governed by a sectoral approach, where specific kinds of sensitive data, like health or financial data, are protected by narrow laws. The result is variation. The Children's Online Privacy Protection Act or COPPA requires that the parent or guardian of a child under the age of 13 must affirmatively opt-in before companies can collect or use their personal information, for example. Other federal laws have chosen to give consumers an opt-out choice. The Gramm-Leach-Bliley Act (GLBA), which includes financial privacy protections, mandates such an opt-out.

With a comprehensive federal privacy law now being discussed, policymakers and advocates have been jostling for an opt-in requirement for all forms of data collection. California Representative Ro Khanna made opt-in a central feature of his Internet Bill of Rights, but admitted that "if you have to click on something 50 times, it kind of defeats the purpose."¹⁶ (Weak opt in, where one click suffices all requirements, contrasts with strong opt in, where consent must be granted for all types of data collection and process.) Internet rights group Access Now made an opt-in an explicit part of their

¹² Rafi Goldberg, "Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds," <https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds>

¹³ American Action Forum, "New AAF Net Neutrality Survey," <https://www.americanactionforum.org/survey/new-aaf-net-neutrality-survey/>

¹⁴ Joseph Farrell, "Can Privacy Be Just Another Good?" http://www.jthtl.org/content/articles/V10I2/JTHTL.v10i2_Farrell.PDF

¹⁵ Keith Tester, "Media Culture, and Morality," https://books.google.com/books/about/Media_Culture_and_Morality.html?id=sa9A9h3ZicAC

¹⁶ Kara Swisher, "Introducing the Internet Bill of Rights," <https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html>

guidelines for lawmakers for the adoption of a new U.S.-wide privacy law.¹⁷ Senior policy counsel at the Open Technology Institute Eric Null has also made the case for an opt-in regime, saying, "The benefit of opt-in is making sure consumer data isn't used in ways they didn't know about, understand, or agree to. Opt-out assumes they know, when in reality we all know they don't. How do you solve that without opt-in?"¹⁸

Null evinces a common and important support for the change to an opt-in regime. The choice, whatever it may be, should be supported by knowledge about the promises and pitfalls of the service. But because consumers don't have that knowledge, they cannot make a prudent decision. So, until consumers know what they are agreeing to, the default must be no collection, many argue.

Many people don't read the terms of service contracts and yet agree to them anyway.^{19,20} One study suggested that only about one in a thousand people click on a site's terms of service.²¹ So there is a tenuous connection *at best* between affirmative consent in agreeing to online services and absolute knowledge of what that consent fully entails. At the heart of the opt-in regime is an affirmative choice that doesn't seem to mean all that much.

Opt-out and opt-in mandates don't differ in their choices or in the kind of information that consumers can access, as will be discussed later. Rather, data collection is a default yes in the case of a privacy opt-out, while the default becomes no for an opt-in regime. What is truly at stake in the opt-in versus opt-out debate then is where the default should be. As Obama's chief regulatory czar wrote of this topic, "setting default options, and other similar seemingly trivial menu-changing strategies, can have huge effect on outcomes." Those outcomes, which affect innovation and jobs, are the reason why an opt-in mandate shouldn't be pursued.

Privacy Preferences

Privacy preferences, like all preferences, tend to be formed at the moment when it is elicited, like when a surveyor asks a question or when a user has to choose among privacy settings. Internet users generally do engage in cost benefit analyses regarding their privacy, but preferences are highly contingent on how survey questions and experimental designs are framed.

The former head of OIRA during the Obama Administration, Cass Sunstein, recently ran an experiment that helps to illustrate some of these framing issues in privacy.²² He asked two groups of people similar questions about the value of Facebook but differed slightly how they were asked.

¹⁷ Access Now, "Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers," <https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf>

¹⁸ Eric Null, <https://twitter.com/ericnull/status/999360346396741632>

¹⁹ Shankar Vedantam, "Do You Read Terms Of Service Contracts? Not Many Do, Research Shows," <https://www.npr.org/2016/08/23/491024846/do-you-read-terms-of-service-contracts-not-many-do-research-shows>

²⁰ Caroline Cakebread, "You're not alone, no one reads terms of service agreements," <https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11>

²¹ Yannis Bakos, Florencia Marotta-Wurgler, and David R. Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443256

²² Cass Sunstein, "How Much Is It Worth to Use Facebook? It Depends," <https://www.bloomberg.com/opinion/articles/2018-05-03/facebook-users-want-to-be-paid-a-lot-to-quit>

The first group was posited, "Suppose that you had to pay for the use of Facebook. How much would you be willing to pay, at most, per month?" The second group, however, was asked: "Suppose that you are being offered money to stop using Facebook. How much would you have to be paid per month, at a minimum, to make it worth your while to stop using Facebook?" For the first question, the median answer was just \$1 per month, while the second question clocked in at a media of \$59 per month. Depending on where the question begins, the value of Facebook can vary widely. That people tend to ascribe more value to things merely because they own them is known as the endowment effect and it is a tendency that has been catalogued throughout decision making.

Decisions regarding privacy are affected by a number of cognitive biases. The benefit of information collection is immediate, in that people get access to a service, while the costs of disclosing that information are delayed. This phenomenon, sometimes called "benefit immediacy," is a time related bias.²³ (It is worth noting that opt-in mandates don't solve this intertemporal problem.)

Due to the conflict between privacy attitudes and actual outcomes, some scholars worry about a privacy paradox.²⁴ As one review of the literature described it, "while many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behavior, this rarely translates into actual protective behavior."²⁵

Indeed, the value of privacy does vary depending on the context. For example, one group of researchers found that the clear majority of customers will buy from a more privacy-invasive firm that was selling DVDs if they offered only a slightly lower price.²⁶ In repeated interactions, this firm got both a larger market share and higher revenue than competitors without data collection. Similarly, professors Christian Happ, André Melzer, and Georges Steffgen found that a over a third of people will readily give up their personal passwords for a bar of chocolate.²⁷ As one seminal study noted, "most subjects happily accepted to sell their personal information even for just 25 cents."²⁸ Using differentiated smartphone apps, economists were able to estimate that consumers were willing to pay a one-time fee of \$2.28 to conceal their browser history, \$4.05 to conceal their list of contacts, \$1.19 to conceal their location, \$1.75 to conceal their phone's identification number, and \$3.58 to conceal the contents of their text messages.²⁹ The average consumer was also willing

²³ David W. Wilson and Joseph S. Valacich, "Unpacking the privacy paradox: Irrational decision-making within the privacy calculus," <https://arizona.pure.elsevier.com/en/publications/unpacking-the-privacy-paradox-irrational-decision-making-within-t>

²⁴ David Ryan Polgar, "RIP, Privacy? The Strange Paradox of How We Act Online," <https://bigthink.com/david-ryan-polgar/the-privacy-paradox-an-interview-with-manoush-zomorodi>

²⁵ Susanne Barth and Menno D.T.de Jong, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," <https://www.sciencedirect.com/science/article/pii/S0736585317302022>

²⁶ Sören Preibusch, Dorothea Kübler, and Alastair R. Beresford, "Price versus privacy: an experiment into the competitive advantage of collecting less personal information," <https://link.springer.com/article/10.1007/s10660-013-9130-3>

²⁷ Christian Happ, André Melzer, and Georges Steffgen, "Trick with treat – Reciprocity increases the willingness to communicate personal data," <https://www.sciencedirect.com/science/article/pii/S0747563216301935>

²⁸ Jens Grossklags and Alessandro Acquisti, "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information," <https://www.econinfosec.org/archive/weis2007/papers/66.pdf>

²⁹ Scott J. Savage and Donald M. Waldman, "The Value of Online Privacy," <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5735f456b654f9749a4afd62/1463153751356/The+value+of+online+privacy.pdf>

to pay \$2.12 to eliminate advertising. Sometimes, consumers are willing to pay a higher price to purchase goods from more privacy-protective merchants.³⁰ Context matters.

Yet, showing users the long-term risks involved in sharing information oftentimes doesn't matter that much for their end choices. Law professors Adam Chilton and Omri Ben-Shahar tested these assumptions within an experiment by simplifying privacy policies and laying out the potential long-term costs of information collection.³¹ They found that these kinds of information changes did little to shift the users' comprehension of the disclosure, the willingness to share personal information, or expectations about their rights.

Similar research only confirms Chilton and Ben-Shahar's result.³² As Brandimarte, Acquisti, and Loewenstein explained after testing privacy disclosure, "the ability of even improved transparency solutions or additional control tools to better align consumer attitudes towards privacy with actual behavior and reduce regret from oversharing is ultimately questionable." In related research, giving users an increased feeling of control over the publication of their data often results in increased and riskier disclosures.³³

Calls for opt-in regulations assume that changing the defaults will help to align privacy preferences with outcomes. But as Daniel Castro and Alan McQuinn point out,

The biannual Eurobarometer survey, which interviews 100 individuals from each EU country on a variety of topics, has been tracking European trust in the Internet since 2009. Interestingly, European trust in the Internet remained flat from 2009 through 2017, despite the European Union strengthening its ePrivacy regulations in 2009 (implementation of which occurred over the subsequent few years) and significantly changing its privacy rules, such as the court decision that established the right to be forgotten in 2014. Similarly, European trust in social networks, which the Eurobarometer started measuring in 2014, has also remained flat, albeit low.³⁴

In other words, it doesn't seem as though strong regulations have done anything to make people feel as though they are getting a better deal with Internet companies. However, social media researchers focused on platform interactions have found that users express increased trust and feelings of control over data when they are more educated about the sites. In one important study on the topic, social scientists discovered that after being told how the Facebook feed works, participants were mostly satisfied with the content on their feeds.³⁵ In a follow up two to six

³⁰ Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti, "Effect of Online Privacy Information on Purchasing Behavior," <https://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf>

³¹ Adam Chilton and Omri Ben-Shahar, "Simplification of Privacy Disclosures: An Experimental Test," https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2443&context=law_and_economics

³² Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency," <http://journals.sagepub.com/doi/abs/10.1177/1948550612455931>

³³ Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, "Misplaced Confidences Privacy and the Control Paradox," <http://journals.sagepub.com/doi/abs/10.1177/1948550612455931>

³⁴ Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use," <http://www2.itif.org/2018-trust-privacy.pdf>

³⁵ Motahhare Eslami and Karrie Karahalios, "Investigating Users' Understanding of Invisible Algorithms and Designing around It," http://social.cs.uiuc.edu/papers/Algorithms_Workshop_ICWSM.pdf

months later, “algorithmic awareness led to more active engagement with Facebook and bolstered overall feelings of control on the site.”

If the move towards an opt-in data regime rests on an information deficit, policy makers might want to consider less onerous options that achieve the same outcomes.

The Privacy Paradox isn't A Paradox

While the privacy paradox often animates calls for regulation, there isn't really a paradox when you dive deeper into decision-making. Just because a person wants privacy doesn't preclude them from also wanting the services and convenience granted from data processing. In an ideal world, users would be able to consume both the service and privacy. But in the real world, users choose in some instances privacy and in other instances to share. Every introductory economics course uses the indifference curve to illustrate how consumption of one good is slowly traded off for the consumption of another. This fundamental insight doesn't stop because the good is intangible like privacy.

A privacy paradox only exists if consumers don't think a trade-off is occurring. Pew found, for example, that “there are a variety of circumstances under which many Americans would share personal information or permit surveillance in return for getting something of perceived value.”³⁶ As those researchers found, many are ok with giving up shopping histories for a discount card but aren't ok when car insurance companies offer cheaper rates if a tracking device is installed. Acxiom and trade group Data & Marketing Association found in their own survey earlier this year that 58 percent of consumers will share personal data under the right circumstances.³⁷

In the most recent survey of its kind, economist Caleb Fuller found that nine out of ten people who use Google are aware of its business practice.³⁸ Moreover, as users consume the service more, they are more aware of the information collection. For those that use Google about once a day, 78 percent are aware of information collection, but this number jumps up for those who use the site “dozens of times a day or more,” to 93 percent. Fuller also found that, “of the 71% of all respondents who said they would prefer not to be tracked, a full 74% are unwilling to pay anything to retain their privacy.”

An unwillingness to pay is a common finding and for good reason. Everyone would love to get something for nothing. Trade association NetChoice worked with Zogby Analytics to find that only 16 percent of people are willing to pay for online platform service.³⁹ Strahilevitz and Kugler found that 65 percent of email users, even though they knew their email service scans emails to serve ads, wouldn't pay for alternative.⁴⁰

³⁶ Lee Rainie, “Privacy and Information Sharing,” <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>

³⁷ Greg Sterling, “Survey: 58% will share personal data under the right circumstances,” <https://marketingland.com/survey-58-will-share-personal-data-under-the-right-circumstances-242750>

³⁸ Caleb S. Fuller, “Is the Market for Digital Privacy a Failure?” https://www.ftc.gov/system/files/documents/public_comments/2017/11/00019-141720.pdf

³⁹ NetChoice, “American Consumers Reject Backlash Against Tech,” <https://netchoice.org/american-consumers-reject-backlash-against-tech/>

⁴⁰ Lior Strahilevitz and Matthew B. Kugler, “Is Privacy Policy Language Irrelevant to Consumers?” https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449

Even still, users take steps to manage their online privacy experiences. A comScore study on cookies found that about 3 in every 10 Internet users delete their cookies every month, a small but powerful sign of interest in privacy.⁴¹ At least a quarter of all US Internet users employ ad blocking technology.⁴² Those aged 18 to 45 are far more engaged.⁴³ Forty five percent of this group enable two-step verification, nearly one third have created another email account dedicated for services, and 17 percent have signed up with security companies to protect their information. Teens use coded language on places like Facebook to maintain privacy from their parents who also might be on the site. While some might claim that people don't know about privacy protection or their setting, three out of four Facebook users are aware of their privacy settings, and even more know how to change their privacy settings, nearly eight in ten.⁴⁴

Part 2 – The Cost of Privacy Regulations

The Cost of Opt-In Versus Opt-Out

Overall, users do care about privacy, take actions to stop data misuse, and are aware of the tools that platforms provide to change their privacy settings. In spite of this positive baselines, could opt-in regulations help educate consumers about the decisions they make?

Rather than educating, opt-in mandates add three big hurdles for consumers as decision makers. First, consumers have substantially less information about decisions they make. Before any additional service can be provided, consumers will have to imagine all of the potential benefits, which will be difficult if not impossible for entrants. The biggest players, however, will be able to make a better case about the benefits. Second, consumers will think that that defaults are suggestions by the company. In other words, they will assume that it is a recommended action, even though they are mandated choices by the government. Lastly, these defaults will become the status quo. Any further change from this baseline will require significant effort by company and will be understood by the decision maker as a trade-off, as psychologists have found.⁴⁵

Consider a system where you have only one option, you can either opt-in or not to data collection before you consume the good or service. If you say yes, then the negotiations have effectively ended. No further choices can be expressed unless you exit from the service completely. The contract is explicit and agreed to upfront. If, however, you are given the choice to opt-out of certain kinds of information processing in the future, then the relationship between you and the provider becomes one of an extended negotiation. Thus, privacy negotiations become a repeated game where a contract is implicitly agreed to but can be modified at some future point.

⁴¹ Gian M. Fulgoni, "Cookie Deletion Rates and the Impact on Unique Visitor Counts," https://www.comscore.com/chi/Insights/Blog/Cookie-Deletion-Rates-and-the-Impact-on-Unique-Visitor-Counts?cs_edgescape_cc=US

⁴² eMarketer, "eMarketer Scales Back Estimates of Ad Blocking in the US," <https://www.emarketer.com/Article/eMarketer-Scales-Back-Estimates-of-Ad-Blocking-US/1015243?ecid=NL1001>

⁴³ Remie Arena, "What Are Consumers Doing to Keep Their Personal Data, Well, Personal?" <https://www.emarketer.com/content/what-are-consumers-doing-to-keep-their-personal-data-well-personal?ecid=NL1001>

⁴⁴ Reuters Poll Data, "Social Media Usage Poll," <http://fingfx.thomsonreuters.com/gfx/rngs/FACEBOOK-PRIVACY-POLL/010062SJ4QE/2018%20Reuters%20Tracking%20-%20Social%20Media%20Usage%205%203%202018.pdf>

⁴⁵ William Samuelson and Richard Zeckhauser, "Status Quo Bias in Decision Making," <https://sites.hks.harvard.edu/fs/rzeckhau/status%20quo%20bias.pdf>

As Nicklas Lundblad and Betsy Masiello explain,

This ought to evolve into an ongoing negotiation and game of repeated trust between the service provider and the user. But what we observe in account-based opt-in decisions is a one-time ex-ante limited choice which applies over the lifetime of a service contract. This actually risks the user's privacy over the long term because the deal requires no further negotiation on the part of the service provider.⁴⁶

Moving data industries to opt-in choices modifies the user's relationship with the processor in a way that changes the relative positions within the negotiation process. Privacy is now, as Haggerty and Ericson explained in 2000, "less a line in the sand beyond which transgression is not permitted, as a shifting space of negotiation where privacy is traded for products, better services or special deals."⁴⁷

The debate over opt-in or opt-out isn't centered around knowledge but around changing the default for consumer preferences. Opt-in defaults show markedly lower participation rates to opt-out defaults even though the good or service is exactly the same. The classic example is organ donation. Although there is widespread support for organ donation, only about 28 percent actually volunteer to be donors, despite the fact that around 85 percent claim to want to be donors. Some countries automatically enroll everyone for organ donation and then allow for opting out, which results in participation rates of 85 percent and higher.

Below is a compendium of studies testing these defaults. Even though consumer options and protections are the same, the default changes participation rates dramatically.

Subject Area	Opt-In Participation Rate	Opt-Out Participation Rate	Source
An on-line survey asking participants if they want to be contacted further about health surveys	48.2 percent	96.3 percent	⁴⁸
Organ donation in Austria		99.98 percent	⁴⁹
Organ donation in Belgium		98 percent	⁴⁶

⁴⁶ Nicklas Lundblad and Betsy Masiello, "Opt-In Dystopias,"

<https://www.scribd.com/document/30469167/Opt-in-Dystopias>

⁴⁷ Kevin D. Haggerty and Richard V. Ericson, "The surveillant assemblage,"

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.9622&rep=rep1&type=pdf>

⁴⁸ Eric J. Johnson, Steven Bellman, Gerald L. Lohse, "Defaults, Framing and Privacy: Why Opting In-Opting Out,"

https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf

⁴⁹ Eric J. Johnson and Daniel Goldstein, "Do Defaults Save Lives,"

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.2319&rep=rep1&type=pdf>

Organ donation in Denmark	4.25 percent		46
Organ donation in France		99.9 percent	46
Organ donation in Germany	12 percent		46
Organ donation in Hungary		99.9 percent	46
Organ donation in Netherlands	27.5 percent		46
Organ donation in Poland		99.5 percent	46
Organ donation in Portugal		99.6 percent	46
Organ donation in Sweden		85.9 percent	46
Organ donation in the United Kingdom	17.2 percent		46

Changing defaults to require that every person affirmatively consents to a data collection service is likely to reduce the total number of people choosing yes, driving down the effectiveness of data processing. For those companies that rely on processing of data, which is increasingly every company, less data will tend to decrease their ability to service consumers. In "The Economics of Privacy," a wide-ranging review of economic research in this space, the authors highlight the trade-offs present in information disclosure,

Individuals can benefit from protecting the security of their data to avoid the misuse of information they share with other entities. However, they also benefit from the sharing of information with peers and third parties that results in mutually satisfactory interactions.⁵⁰

A reduction in the exchange of data isn't welfare enhancing. Opt-in privacy regimes have been tried before in the United States and were found to be costly. In a court case with US West, a telephone company that is now part of CenturyLink, it was revealed that obtaining permission to sell their services cost the company between \$21 and \$34 per consumer.⁵¹ By their own internal calculations,

⁵⁰ Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," https://www.ftc.gov/system/files/documents/public_comments/2017/10/00006-141501.pdf

⁵¹ Julie Tuan, "U.S. West, Inc. v. FCC,"

<https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1276&context=btl>

US West had to make 4.8 calls to each customer household before they reached an adult who could grant consent to share information. In one-third of households called, U.S. West never reached the customer. Altogether, customers received more calls from the opt-in regime than in an opt-out system even though many weren't able to enjoy the benefits of new services.

In other industries where opt-in regimes have been imposed, studies have found higher costs and slowed innovation. A 2000 Ernst & Young study of financial institutions found that these mandates cost the entire industry \$56 billion.⁵² For charities, the cost of compliance with an opt-in privacy law would have been nearly 21% of their total revenue.⁵³ In contrast, industry estimates from the American Banker suggest that around 5 percent of people choose to opt out of sharing financial information under GLBA requirements, a significantly smaller impact.⁵⁴

The implementation of the General Data Protection Regulation (GDPR) in Europe at the end of May should serve as a stark warning to policymakers here in the United States as it is an opt-in privacy regime. Early research on the regulatory impact of the GDPR find that the biggest players have been able to weather the storm while smaller firms have been wiped out.⁵⁵ Smaller advertising firms have lost between 28 and 32 percent of their placements on web sites, while Google was able to increase their web presence by 1 percent. Economists focused on privacy predicted exactly this result years earlier.⁵⁶

While the rule change with GDPR is still recent, earlier privacy regulation in Europe suggests that the impact on small sites could be massive. The implementation of restricted information sharing rules under e-Privacy decreased the efficacy of advertising by 65 percent relative to the rest of the world, cutting off the lifeblood of Internet startups.⁵⁷ Those hardest hit were general content sites like news outlets. The cost of privacy regulation is one of the reasons why Europe lags in startups.

The Cost of GDPR and Other Privacy Regimes

The early costs involved with GDPR compliance hints at the costs that United States industries would face if a broad privacy law were implemented. Importantly, the GDPR imposes three kinds of costs on firms. First, the regulation forces firms to retool data processes to realign with the new demands. This is generally one-time fixed cost that raises the cost of all information using entities. Second, the regime adds risk compliance costs, causing companies to staff up to ensure compliance. Finally, the law will change the investment dynamics for all those affected industries.

Currently, the retooling costs and the risk compliance costs are going hand in hand, so it is difficult to suss out the costs of each. Still, they are substantial. A McDermott-Ponemon survey on GDPR preparedness found that almost two-thirds of all companies say the regulation will "significantly

⁵² Cynthia Glassman, "Customer Benefits from Current Information Sharing by Financial Services Companies"

⁵³ Fred Cate, "The Privacy Problem,"

<https://web.archive.org/web/20150912045126/http://www.firstamendmentcenter.org/madison/wp-content/uploads/2011/03/FirstReportprivacyproblem.pdf>

⁵⁴ W.A. Lee, "Opt-Out Notices Give No One a Thrill," <https://www.americanbanker.com/news/opt-out-notices-give-no-one-a-thrill>

⁵⁵ Björn Greif, "Study: Google is the biggest beneficiary of the GDPR" <https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr>

⁵⁶ James Campbell, Avi Goldfarb, and Catherine Tucker, "Privacy Regulation and Market Structure," <https://onlinelibrary.wiley.com/doi/abs/10.1111/jems.12079>

⁵⁷ Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259

change" their informational workflows.⁵⁸ For the just over 50 percent of companies expecting to be ready for the changes, the average budget for getting to compliance tops \$13 million, by this estimate. Among all the new requirements, this survey found that companies were struggling with the data-breach notification the most. The inability to comply with the notification requirement was cited by 68 percent of companies as posing the greatest risk because of the size of levied fines.

The International Association of Privacy Professionals (IAPP) estimated the regulation will cost Fortune 500 companies around \$7.8 billion to get up to speed with the law.⁵⁹ And these won't be onetime costs since, "Global 500 companies will be hiring on average five full-time privacy employees and filling five other roles with staff members handling compliance rules." A PwC survey on the rule change found that 88 percent of companies surveyed spent more than \$1 million on GDPR preparations, and 40 percent more than \$10 million.⁶⁰

It might take some time to truly understand the impact of GDPR, but the law will surely change the dynamics of countless industries. For example, when the EU adopted the e-Privacy Directive in 2002, Goldfarb and Tucker found that advertising became far less effective.⁶¹ The impact seems to have reverberated throughout the ecosystem as venture capital investment in online news, online advertising, and cloud computing dropped by between 58 to 75 percent.⁶² Information restrictions shift consumer choices. In Chile, for example, credit bureaus were forced to stop reporting defaults in 2012, which was found to reduce the costs for most of the poorer defaulters, but raised the costs for non-defaulters.⁶³ Overall the law led to a 3.5 percent decrease in lending and reduced aggregate welfare.

In the United States, because of differences in the roll out of electronic health records, two professors, Amalia Miller and Catherine Tucker, were able to test the impact of state privacy regulations on health outcomes.⁶⁴ Their analysis put a number on the cost privacy applies to EMR adoption. Privacy laws reduced adoption by some 24 percent. Why is this important? Better health data leads to better understanding of patients and typically better outcomes. Live are on the line, since a 10 percent increase in the adoption of such systems can reduce infant mortality by 16 deaths per 100,000 births.

Conclusion

⁵⁸ Ashley Winton, Larry Ponemon, and Mark E. Schreiber, "New study highlights lack of GDPR preparedness," <https://iapp.org/news/a/new-study-highlights-lack-of-gdpr-preparedness/>

⁵⁹ Daily Dashboard, "Global 500 companies to spend \$7.8B on GDPR compliance,"

<https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/>

⁶⁰ PwC, "Pulse Survey: GDPR budgets top \$10 million for 40% of surveyed companies,"

<https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html>

⁶¹ Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising,"

<https://pubsonline.informs.org/doi/abs/10.1287/mnsc.1100.1246>

⁶² Anja Lambrecht, "E-Privacy Provisions and Venture Capital Investments in the EU,"

<https://www.ceps.eu/sites/default/files/E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments%20in%20the%20EU.PDF>

⁶³ Andres Liberman, Christopher Neilson, Luis Opazo, and Seth Zimmerman, "The Equilibrium Effects of Information Deletion: Evidence from Consumer Credit Markets," <https://www.nber.org/papers/w25097>

⁶⁴ Amalia R Miller and Catherine E. Tucker, "Can Healthcare IT Save Babies?"

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1080262

In a zeal to ensure that consumers express their true preferences, opt-in mandates tax the exchange of data. Since privacy valuations are both contextual and highly personal, there is no guarantee that opt-in will yield the right balance between innovation and default protection. As detailed throughout this comment, opt-in regimes don't lead to an optimal level of privacy.

Further, privacy regulations impose real costs on the economy, on innovation, and on real lives. Those who are engaged in the policy discussion and who believe in strong privacy regulations shouldn't be dismissing that costs occur. Rather, they should be upfront with what they are willing to sacrifice for more data control.



**COUNCIL for
CITIZENS
AGAINST
GOVERNMENT
WASTE**

Thomas A. Schatz, *President*
1100 Connecticut Ave., N.W., Suite 650
Washington, D.C. 20036
ccagw.org

February 25, 2019

The Honorable Frank Pallone
Chairman
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Greg Walden
Ranking Member
Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

Janice D. Schakowsky
Chairman
Subcommittee on Consumer Protection
& Commerce
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Cathy McMorris-Rogers
Ranking Member
Subcommittee on Consumer Protection
& Commerce
Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Pallone, Ranking Member Walden, Chairman Schakowsky, and Ranking Member McMorris-Rogers:

On behalf of the more than one million members and supporters of Citizens Against Government Waste (CCAGW), I offer the following comments and recommendations on ways to advance consumer privacy while protecting prosperity and innovation for submission to the record for the February 26, 2019 hearing on "Protecting Consumer Privacy in the Era of Big Data:"

Policymakers and individual Americans have become increasingly concerned about the amount of personal information held by online platforms, e-commerce sites, internet service providers (ISPs), banking institutions, retailers and many others, and how such information is being used for data analytics, online advertising, and targeted messaging without adequate transparency or consumer choice by social media companies and online search engines. This concern was underscored after the 2016 elections when it was revealed that Cambridge Analytica used ill-gotten personal data for targeted political ads.

Furthermore, new technologies, including automated license plate readers, event data recorders in vehicles, and radio frequency identification, are making it easier to track, collect, access, and repurpose or manipulate personal information.

The United States has enacted several laws that contain provisions governing how personal information should be protected using an industry-by-industry approach, including the Communications Act of 1934, the Electronic Communications Privacy Act, the Children's Online Privacy Protection Act, the Driver Privacy Act, the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Health Insurance

Portability and Accountability Act, the Wire Act, and the Video Privacy Protection Act. There is no single law or federal agency for protecting consumer privacy. The most prominent agency entrusted with protecting consumer privacy are the Federal Trade Commission (FTC).

On April 14, 2016, the European Parliament adopted the General Data Protection Regulation (GDPR). The GDPR entered into force on May 24, 2016, and its provisions became directly applicable to all member states on May 25, 2018. The GDPR imposes requirements for data protection by businesses or other entities that process the personal data of individuals in the member states of the European Union, regardless of where the data processing takes place.¹ This includes U.S. companies conducting business in the E.U. These U.S. companies need to be able to rely on a U.S. framework that facilitates trade and data transfer around the world, including with Europe.

On June 28, 2018, the California Consumer Privacy Act was signed into law by Governor Jerry Brown. The bill, which was rushed through the legislature in a few days, imposes extremely onerous requirements on how companies must store and provide access to consumers' personal information, as well as harsh restrictions on the types of product and service options and discounts companies may offer to their customers. Other states have enacted or are reviewing laws that would purportedly protect personal information, covering issues such as children's online privacy, website privacy policies, and monitoring employee e-mail communications. There is an overriding concern that without the adoption of a consistent national privacy protection regime that preempts state and local laws, more states will follow California's example, further complicating the privacy regulatory environment that companies, large and small, must negotiate.

CCAGW offers the following recommendations for consumer-based privacy:

1. National Privacy Framework: Because of the unique nature of the internet ecosystem and its presence beyond state borders, a clear and concise national data privacy framework is necessary to provide consistency and certainty for businesses and consumers alike.
2. Consumer Choice and Control: Businesses should provide consumers with easy-to-understand privacy choices based on the sensitivity of their personal data and how it will be used or disclosed, consistent with the FTC's privacy enforcement guidance. Businesses should provide consumers with an opt-out choice to use their non-sensitive customer information for personalized third-party marketing. Businesses should be able to continue to rely on implied consent to use customer information for activities such as service fulfillment and support, fraud prevention, market research, product development, network management and security, compliance with the law, and first-party marketing.
3. Transparency: Consumers should be provided with clear, comprehensible, accurate, and continuously available privacy notices by businesses collecting, using, or sharing consumer data that describe in detail the information being collected, how that information will be used, and whether the information will be sold or shared with third

¹ Roslyn Layton, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," *Federalist Society Review*, Volume 19, October 29, 2018, <https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course>.

parties. Should customer information be sold or shared with a third party, customers must be notified about the types of third parties to whom their information has been given and for what purpose.

4. Data Minimization and Contextuality: Consumers should expect reasonable limits on the amount of personal data that organizations will collect, use, and disclose, consistent with the context in which that data is provided. Every effort should be made to de-identify and delete data as promptly as possible when it is no longer necessary.
5. Flexibility: Different types of data require separate methods and standards of protection. For example, sensitive health care data and financial data require a higher level of security than a social media account or a computer's IP address. Therefore, policies must be consistent with the type of data being collected and how it is to be used.
6. Data Security and Breach Notification: Consumers should expect that the personal data they share with other entities is maintained in a secure environment. Information technology systems are under constant attack; breaches have and will continue to occur. In the event of a data breach in which there is a reasonable likelihood of misuse and consumer harm, consumers should expect timely notification of the event, and an offer by the entity breached as to the remedies available to make the consumer as whole as possible, including credit protection services, fraud alerts, and credit monitoring through credit reporting agencies.

We appreciate the opportunity to provide you with our views and recommendations. If you have any questions or concerns, please feel free to contact either myself, or CCAGW Technology and Telecommunications Policy Director Deborah Collier at (202) 467-5300. Thank you.

Sincerely,





United States Congress
House Committee on Energy and Commerce
Subcommittee on Consumer Protection & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

February 26, 2019

Dear Chairwoman Schakowsky and Ranking Member McMorris Rodgers:

The Coalition for a Secure and Transparent Internet (CSTI) writes to thank you for your leadership on the Energy and Commerce Subcommittee on Consumer Protection and Commerce. In response to the hearing being held today, titled "Protecting Consumer Privacy in the Era of Big Data" we write to encourage the subcommittee to do all you can to protect consumers' privacy by restoring open access to WHOIS registration data. An open and accessible WHOIS is critical to protecting Internet users from online criminal activity and to enabling action against network and cyber security risks, illegal online opioid sales, human trafficking, consumer fraud and abuse as well as intellectual property violations.

WHOIS data is the publicly available information on who has registered and administers generic top level domain (gTLDs) names in spaces like .com and .net as well as certain country-code domain spaces like .TV. WHOIS data has been publicly accessible for free since the inception of the Domain Name System. Generic top-level domain name registrars and registries are contractually required to collect contact information from all domain name registrants at the time of registration. This contact data, including name, address, phone number, and email address, is combined with certain other attributes of a domain name's registration to comprise WHOIS data. Accessible WHOIS data is important to law enforcement and regulators tasked with protecting consumers. Such data provides information about who may operate illegal sites, common connections between suspect sites, and the identity of Internet Service Providers to contact for additional evidence.

Due to an overly broad interpretation of the EU's General Data Protection Regulation (GDPR), many domain name registrars and registries are shutting down public access to the full range of WHOIS data, both for one-off requests and automated access. Though the GDPR intended to create privacy protections for consumers, the current interpretation has ironically only strengthened protections for internet criminals. Law enforcement, consumer protection agencies, child advocacy groups, anti-human trafficking organizations, cybersecurity investigators, copyright and trademark holders, journalists, academics, and others rely on WHOIS to help determine *who is* operating a criminal website, sending malicious (SPAM, phishing) emails, or initiating cyber security attacks.

Private citizens are not the only constituency affected by a redacted WHOIS; numerous government agencies rely on WHOIS to conduct their criminal investigations. As Dan Burke, Senior Operations Manager, Cybercrime Investigations Unit of the U.S. Food & Drug Administration, testified before a hearing held by the Senate Caucus on the International Narcotics Control, the lack of access to WHOIS data is impairing the FDA's efforts to combat the illegal online sales of opioids:

"Conducting online investigations is not easy, and FDA has a narrow, but important role in combatting the online sale of opioids. For good or bad, much of the Internet ecosystem,

including dark nets, have adapted and changed to build in anonymity. Public information about the owner of a domain name, known as “whois” data, is now often impossible to access with the implementation of the GDPR.”¹

In short, when WHOIS data goes dark it takes away a critical source of information that is used to help keep the internet safe, secure and sustainable for all internet users.

We encourage the Subcommittee consider legislation that would restore this vital asset for law enforcement and cyber security experts. CSTI and our member organizations look forward to working with you to continue protecting consumers online.

Thank you again for your time and attention to this important issue.

Sincerely,

The Coalition for a Secure and Transparent Internet
www.SecureandTransparent.org

ACT | The App Association; Alliance for Safe Online Pharmacies; Coalition for Online Accountability; Crucial Point LLC; CTO Vision; DomainTools; LegitScript; Liberty Asia; Motion Picture Association of America; National Association of Boards of Pharmacy; National Cyber-Forensics and Training Alliance; Partnership for Safe Medicines; Recording Industry Association of America

¹ <https://www.drugcaucus.senate.gov/sites/default/files/FDA%20Testimony%20on%20Fentanyl%20final.pdf>



1212 New York Ave. NW,
Suite 900
Washington, DC 20005
202.525.5717

Free Markets. Real Solutions.
www.rstreet.org

February 26, 2019

The Honorable Janice D. Schakowsky, Chairwoman
Subcommittee on Consumer Protection and Commerce
Energy and Commerce Committee
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers, Ranking Member
Subcommittee on Consumer Protection and Commerce
Energy and Commerce Committee
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, D.C. 20515

RE: Hearing on "Protecting Consumer Privacy in the Era of Big Data"

Dear Chairwoman Schakowsky & Ranking Member McMorris Rodgers:

We at the R Street Institute ("R Street") commend you and the Subcommittee for holding this hearing on "Protecting Consumer Privacy in the Era of Big Data."¹ Given the changing nature of the economy and recent legal developments, both abroad and among the various states, a comprehensive review of the United States' approach to consumer privacy is both appropriate and timely.

R Street's mission is to engage in policy research and outreach to promote free markets and limited, effective government. As part of that mission, R Street has researched and commented upon multiple policy issues relating to consumer privacy. Recent comments provided to the National Telecommunications and Information Administration aptly summarized this work.² A full review of that work is beyond the scope of this hearing, but we offer the following points to guide the Subcommittee's examination of these important issues:

¹ *Hearing on 'Protecting Consumer Privacy in the Era of Big Data' Before the House Committee on Energy & Commerce*, 116th Cong. (Feb. 26, 2019), <https://goo.gl/r5aGPo>.

² Charles Duan et al., "Comments of R Street Institute," *In re Developing the Administration's Approach to Consumer Privacy*, No. 180821780-8780-01 (Nov. 9, 2018), <https://goo.gl/6Ydgmt>.

The Honorable Janice D. Schakowsky
The Honorable Cathy McMorris Rodgers
February 26, 2019
Page 2

Only Congress can establish a uniform national privacy framework.

Motivated by recent legislation in California and elsewhere, there have been increasing calls for a national privacy framework to preempt state laws and establish uniform privacy protections throughout the United States. The Federal Trade Commission (“FTC”) has the ability to make privacy rules under its general consumer-protection rulemaking authority³—as privacy abuses are surely now “prevalent” enough to satisfy the demands of (b)(3)⁴—but they would merely set a floor, not a ceiling. Such rules would preempt state laws that conflict with or frustrate the purpose of the federal framework, but would likely not preempt state laws that go above and beyond the federal framework, potentially leaving consumer privacy protections inconsistent from state to state. Thus, if Congress wants to establish a national framework that preempts the field and establishes truly uniform privacy protections, it must take action.

Data privacy and competition issues are intertwined.

When properly balanced, the relationship between data privacy and competition is symbiotic—with strong consumer protections that promote fair competition and in turn promote innovation and consumer welfare. But pushing too far in either direction may generate harms that far outweigh any benefits. For example, laws like the General Data Protection Regulation in Europe may offer stronger privacy protections for consumers, but they may also impose costs on industry that are ultimately manifested in higher prices, increased consolidation and reduced innovation. Similarly, prohibiting certain data-driven business models or practices may result in higher prices and fewer choices for consumers. Thus, when considering any potential changes to the current privacy framework, Congress should recognize that data privacy and competition issues are intertwined. Protecting consumer privacy in the era of big data will require a careful balance between the two.

Existing institutions can be improved significantly.

Before making wholesale changes to the current privacy framework, Congress should first try to identify the strengths and weakness of the current approach and look for ways to make incremental improvements. For example, commenters have criticized the FTC for relying too heavily on consent decrees and failing to provide adequate guidance for industry or redress for affected consumers. Many of these criticisms could be addressed through internal process reforms and additional appropriations.⁵ Additional staff for the Bureau of Consumer Protection’s Privacy and Identity Protection Division would surely help, and the role of state attorneys general should not be discounted. A uniform federal framework would necessarily limit the influence that state legislatures wield over consumer privacy, but it could also utilize the resources and experience of state attorneys general to supplement and reinforce efforts at the federal level. These ideas deserve

³ 15 U.S.C. § 57a.

⁴ 15 U.S.C. § 57a(b)(3).

⁵ See, e.g., Tom Struble, “Reforming the Federal Trade Commission Through Better Process,” *R Street Policy Study No. 122* (Dec. 2017), <https://goo.gl/ZwvDdd>.

The Honorable Janice D. Schakowsky
The Honorable Cathy McMorris Rodgers
February 26, 2019
Page 3

thorough consideration, as the optimal framework for consumer privacy must efficiently utilize all available resources.

Any grant of new authority should be carefully limited.

The debate over consumer privacy covers a wide variety of issues, but Congress should try to focus its review on specific harms and practices that are not adequately covered by existing law. History shows that unbounded administrative rulemaking authority can cause serious problems for both industry and consumers,⁶ so any grant of new authority to the FTC (or any other agency) should be carefully limited in order to minimize the potential for future abuse.

* * *

We again commend you for your efforts to protect consumer privacy. We look forward to working with you and the rest of the Subcommittee as you consider potential legislation in this area.

Sincerely,

Charles Duan, Technology and Innovation Policy Director
R Street Institute

Sasha Moss, Federal Government Affairs Manager
R Street Institute

Tom Struble, Technology and Innovation Policy Manager
R Street Institute

Jeff Westling, Technology and Innovation Policy Associate
R Street Institute

CC:

The Honorable Frank Pallone, Chairman
The Honorable Greg Walden, Ranking Member

⁶ J. Howard Beales, Fed. Trade Comm'n, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (May 30, 2003), <https://goo.gl/TZX9sl>.



Tim Day
Senior Vice President
U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062

February 25, 2018

The Honorable Janice D. Schakowsky
Chair
Subcommittee on Consumer Protection
and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection
and Commerce
U.S. House of Representatives
Washington, DC 20515

Re: Hearings on Competition and Consumer Protection in the 21st Century (P181201)

Dear Chair Schakowsky and Ranking Member McMorris Rodgers:

The U.S. Chamber of Commerce respectfully submits this letter for the record for the hearing entitled "Protecting Consumer Privacy in the Era of Big Data," and commends the Subcommittee for taking the lead in bringing together stakeholders to address this critically important issue.

The Chamber recognizes the importance of consumer privacy and, for this reason, we recently released model data privacy legislation,¹ which includes a nationwide privacy framework to protect privacy based upon risk to consumers, encourages transparency, and promotes innovation through collaboration between government and private stakeholders. We believe you should move forward with legislation that draws upon the principles as incorporated in the model legislation.

I. A National Privacy Framework is Necessary

The Chamber believes a new privacy approach is necessary. In light of high-profile incidents surrounding data, the implementation of the General Data Protection Regulation ("GDPR") in Europe and passage of the California Consumer Privacy Act ("CCPA") as well as pending legislation in other states the Chamber urges Congress and the Administration to enact federal privacy legislation that offers consistent protections to Americans and promotes "harmonization and interoperability nationally and globally."²

¹ See U.S. Chamber of Commerce Model Privacy Bill (February 13, 2019) available at https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf.

² 83 Fed. Reg. 48600.

Tim Day, USCC

Last year, California enacted the nation's first comprehensive privacy law. Among other things, the law requires companies to honor consumers' requests to stop selling personal information about them (also known as "opt-out" consent) and mandates that companies disclose to consumers the types of data about them that are sold.³ The law will not be enforced until six months after California's Attorney General publishes regulations, or July 1, 2020, whichever comes first.⁴

California is not alone in enacting privacy laws. Other states have enacted laws that affect individual sectors of the economy or practices not currently specifically addressed by a federal privacy law. For example, in May, the state of Vermont enacted a data privacy and security bill that covers data brokers.⁵ The Illinois' Biometric Information Privacy Act ("BIPA") prohibits the disclosure or use of biometric information without written consent.⁶ These often conflicting regimes, and the possibility that other states will also pass privacy laws, creates regulatory uncertainty which is harmful for businesses and confusing for consumers, who would have to understand and interact with many conflicting regimes.

Given the impact of data on interstate commerce and US economic prosperity, today's current technological and state regulatory environment necessitates a federal privacy law that preempts state and local privacy laws. A national privacy framework also will bolster continued U.S. leadership in trade internationally and facilitate interoperable cross-border data transfer frameworks. Policies that promote the free flow of data across state and national borders will facilitate numerous consumer benefits, economic growth, and trade.

In addition to creating regulatory certainty, a national federal privacy law would also be legally appropriate. Congress has long had the power to regulate both the instrumentalities and channels of interstate commerce as well as activities that substantially affect interstate commerce.⁷ In today's e-commerce environment, consumer data acquired during a purchase order may be transmitted from a computer in Virginia over an interstate broadband network to one of nearly 3 million data centers scattered across the country.⁸ This data can then be used to alert product fulfillment and shipping in yet another state like Tennessee.

³ SB 1121, the California Consumer Privacy Act (Signed into law September 23, 2018) available at https://leginfo.ca.gov/pub/09_2018/bills_001_0100_0000_0100_0000_bill_201720180SB1121.html.

⁴ *Id.*

⁵ See Act 171 (Enacted into Law May 22, 2018) available at <https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf>.

⁶ See 740 ILL. COMP. STAT. 14/15. Unfortunately, some plaintiffs have attempted to extend the reach of BIPA beyond Illinois itself. See Brief for the Chamber of Commerce of the United States of America as *Amicus Curiae* in Support of the Petitioner, *Patel v. Facebook, Inc.*, No. 3:15-cv-03747 (May 7, 2018) available at <http://www.chamberlitigation.com/sites/default/files/cases/files/18181818/U.S.%20Chamber%20Amicus%20Brief%20-%20Patel%20v.%20Facebook%20Inc.%20%28Ninth%20Circuit%29.pdf> Some companies, as a result of BIPA have decided to stop offering some services in Illinois as well. Amy Korte, "Privacy Law Prevents Illinoisans from Using Google App's Selfie Art Feature," *Illinois Policy* (Jan. 23, 2018) available at <https://www.illinoispolicy.org/privacy-law-prevents-illinoisans-from-using-google-apps-selfie-art-feature/>.

⁷ *United States v. Lopez*, 514 U.S. 549 (1995).

⁸ See Chamber Technology Engagement Center, "Data Centers: Jobs and Opportunities in Communities Nationwide," at 4 (2017) available at https://www.uschamber.com/sites/default/files/ctec_datacentertrpt_lowres.pdf.

Tim Day, USCC

Not only does the current e-commerce environment make the handling of consumer data inherently an interstate issue, the value of the digital economy has a significant effect on the national economy and the welfare of individual Americans. For example, according to one study, digital advertising will overtake other forms of ads this year, topping over \$100 billion in value.⁹

Data-driven services are beneficial to consumers. For example, the vast majority of Americans prefer targeted advertising.¹⁰ Revenues obtained by providers from advertisers help reduce prices consumers must pay for products and services.¹¹ Financial services companies are now using data to widen the pool of applicants that have access to credit.¹²

In the future, autonomous vehicles, which have the potential to reduce the 40,000 road fatalities each year (of which 94 percent are caused by human error)¹³ will potentially use and transmit up to 4 terabytes of data per day.¹⁴

The 5G networks that will transfer the mass amounts of data necessary to power smart cities and the Internet of Things could produce over 3 million new jobs and \$500 billion in increased GDP over the next decade.¹⁵

II. Creating and Enforcing a New Federal Privacy Framework

A. What Outcomes Should Arise from a New Consumer Privacy Approach

Policymakers should continue to focus on consumer data. The Chamber believes that a national privacy approach should be risk-focused. Privacy protections should be considered in light of the benefits provided to consumers and the economy and the privacy risks presented by the data being used, and the way a business uses it. Federal enforcement agencies should focus on cases in which consumers suffer actual harm, as opposed to mere speculative injuries or technical violations of the law. The Chamber's privacy legislation discussion draft draws upon these principles.

⁹ Sean Fleming, "Digital now accounts for half of all US advertising," World Economic Forum (Oct. 18, 2018) available at <https://www.weforum.org/agenda/2018/10/digital-now-accounts-for-half-of-all-us-advertising/>.

¹⁰ See IAB, "The Value of Targeted Advertising to Consumers," (citing 2016 survey stating 71 percent of consumers prefer targeted advertising) available at <https://www.iab.com/wp-content/uploads/2016/05/Value-of-Targeted-Ads-to-Consumers2.pdf>.

¹¹ Laurence Green, "Does advertising increase consumer prices?" Advertising Association, available at <https://www.adassoc.org.uk/advertisings-big-questions/does-advertising-increase-consumer-prices/>.

¹² Ann Carnns, "New type of credit score aims to widen pool of borrowers," *The Seattle Times* (Nov. 3, 2018) available at <https://www.seattletimes.com/business/new-type-of-credit-score-aims-to-widen-pool-of-borrowers/>.

¹³ See Chamber Technology Engagement Center Comments to Department of Transportation at 1-2, *In the Matter of Automated Vehicle Policy Summit* (Mar. 9, 2018) available at https://www.uschamber.com/sites/default/files/c_tec_av_3.0_comments_1.pdf.

¹⁴ Kathy Winter, "Meaning Behind One Big Number: 4 Terabytes," Intel Newsroom (Apr. 14, 2017) available at <https://newsroom.intel.com/editorials/self-driving-cars-big-meaning-behind-one-number-4-terabytes/>.

¹⁵ See Accenture Strategies, "Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities," at 1 (2017) available at https://www.accenture.com/t20170222T202102_w_us-en/_acnmedia/PDF-43/Accenture-5G-Municipalities-Become-Smart-Cities.pdf.

Tim Day, USCC

Consumers should have a say as to how personally identifiable information about them is shared. That is why the Chamber's model legislation offers consumers the ability to opt out of data sharing with third parties. At the same time, companies using and sharing consumer data should be able to continue innovating and not be hindered by consumer consent outcomes and regulations that do not take into consideration the risks and benefits of data.

Consumers, upon verified request, should be given the qualified ability to request information about them be deleted. Any proposed right of deletion, like the CCPA, must allow for reasonable exceptions to such requests. Data deletion rights though should not impede a company's ability to among other things to provide the goods or services for which a consumer and business contract, maintain good data hygiene, conduct security-protected research, combat fraud and security threats, and comply with legal obligations.

B. Accountability

1. Government Enforcement

The Chamber recognizes that robust privacy laws already apply to many sectors of the economy.¹⁶ Policymakers should work to harmonize sectoral privacy approaches unless there is a meaningful reason to keep an existing sectoral law. While the Chamber believes that some sectoral privacy laws dealing with sensitive personal information, such as the Health Insurance Portability and Accountability Act ("HIPAA"), should remain in place, policymakers and stakeholders should continue to engage industry about how legacy privacy laws interact with a new national privacy framework. Any new privacy framework should not impose dual enforcement of multiple federal agencies upon regulated entities.

With a few statutorily-established sectoral exceptions, the U.S. Chamber of Commerce recognizes that the Federal Trade Commission ("FTC" or "Commission") generally is best positioned to enforce a new federal privacy framework. The FTC, pursuant to its Section 5 Unfair and Deceptive Trade practices authority in the FTC Act, has taken enforcement actions against various entities for privacy related issues. Additionally the FTC has "enforced statutes that protect certain health, credit, financial, and children's information" and has "brought over 500 cases protecting the privacy and security of consumer information."¹⁷ It is clear for those sectors within its established jurisdiction that the FTC has the expertise to enforce any new federal privacy framework. For this reason, the Chamber proposes that FTC be given the increased "unfair and deceptive trade practices" authority to enforce new consumer privacy rights such as opt-out, deletion, and transparency.

¹⁶ For example, sectoral federal privacy laws apply to entities in the healthcare, financial, insurance, and communications sectors. Other companies, like transportation companies, while not regulated specifically under a federal privacy law are under the jurisdiction of agencies like the Department of Transportation.

¹⁷ See Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission at 4, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27, 2016) available at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

Tim Day, USCC

2. Private-Sector Based Accountability

The private sector must also establish practices to promote accountability for businesses. While many companies are already transparent with their consumers, the Chamber supports requiring companies to be transparent with consumers about the collection, use, and sharing of information and to provide this information to consumers in an easily-accessible format. Consumers should be able to obtain information regarding the ways in which personally identifiable information about them is collected, used, and disclosed. These transparency efforts should provide consumers meaningful information without hampering legitimate businesses practices and inundating individuals with information overload.

The private sector and federal regulators should also work in a collaborative and not adversarial manner and should establish partnerships to develop methods for achieving consumer privacy outcomes. For example, federal enforcers should not focus on taking enforcement actions against companies acting in good faith that have made technical violations of privacy statutes.

Any federal privacy law should provide safe harbor provisions that enable companies following agency-approved guidelines to be in compliance with federal law. For example, the Children's Online Privacy Protection Act provides for such a program in which the FTC approves regulatory guidelines after notice and comment.¹⁸ The Chamber's bill relies on the statutory language of COPPA's Safe Harbor Program.

III. Encouraging Privacy Innovation

In addition to the establishment of policy outcomes that will be promoted by the private sector and enforced by appropriate government regulators, policymakers should also recognize the value that technology can play in working to protect the privacy of consumers. Any privacy approach should be technology-neutral and not favor one technological solution over another in achieving desired outcomes.

Congress should consider the role that technology plays in assessing risk to consumers regarding privacy and security. For example, several companies are working to use technology to assess security practices in order to protect information about consumers.¹⁹ The Administration should not endorse any particular technological solution or approach, but it can – and should – facilitate innovative approaches to addressing consumer privacy.

Technologies such as blockchain also hold the promise of securely transmitting information. Blockchain uses cryptographic methods to support secured transactions ranging from applications such

¹⁸ See e.g., 15 U.S.C. § 6503.

¹⁹ See, e.g., Andrew Ross, "Fico release free cyber security ratings service to companies worldwide," Information Age (June 19, 2018) available at <https://www.information-age.com/fico-cyber-security-rating-123473126/>; Brian Nordli, "How engineers at NSS labs put the 'security' in cybersecurity," Built in Austin (May 30, 2018) available at <https://www.builtinaustin.com/2018/05/30/NSS-Labs-Engineering-Spotlight>.

Tim Day, USCC

as food security in supply chains²⁰ to real estate title transfer.²¹ Congress and the Administration should encourage technologies like blockchain by fostering a regulatory environment that enables innovation to thrive.

IV. Conclusion

Data is important to every business in the United States whether it be credit reporting companies enabling consumers to be able to access credit in a matter of minutes as opposed to days, marketers presenting tailored products and services to consumers, or automakers and technology firms contributing to the reduction of traffic deaths. Effective, innovative, and responsible use of data is improving the lives of Americans in significant ways. Large amounts of data are being used, analyzed, and shared to bring about these positive societal and economic changes, and companies must respect the privacy of individuals.

In order to achieve the right regulatory balance that strives to protect consumer privacy, foster regulatory certainty, and promote innovation, Congress, and the Administration must work to develop a federal privacy law that establishes a consistent national standard and avoids a patchwork of federal and state regulations.

The Chamber stands ready to work with the Subcommittee to help develop a national privacy framework that benefits all Americans.

Sincerely,



Tim Day
Senior Vice President

CC: The Honorable Frank Pallone, The Honorable Greg Walden

²⁰ Brigid McDermott, "Improving Confidence in Food Safety with IBM Blockchain," (Sept. 5, 2017) available at <https://www.ibm.com/blogs/blockchain/2017/09/improving-confidence-in-food-safety-with-ibm-blockchain/>.

²¹ Don Oparah, "3 Ways that Blockchain will Change the Real Estate Market," Tech Crunch (Feb. 6, 2016) available at <https://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/>.



February 25, 2019

House Energy & Commerce
Subcommittee on Consumer
Protection & Commerce
2123 Rayburn HOB
Washington, DC, 20515

Dear Members of the Subcommittee on Consumer Protection & Commerce:

Thank you for the opportunity to submit comments for the record regarding your hearing on "Protecting Consumer Privacy in the Era of Big Data." This submission suggests a method that could be used to address consumer data privacy.

The market for user data is a relatively new marketplace where individuals are affected by a company's practices, but those individuals are not the company's customers. Because the user is not the customer, companies may not be entirely responsive to the requests or needs of their users in the same way that they are responsive to their customers. The following ideas could offer a targeted mechanism to promote privacy principles in the marketplace.

There is a distinction between companies that sell products to users and companies that sell user data or advertising to users.

Within this context, guidance for another category of personal data – user-controlled data – could be helpful. For example, activities that fall into the user-controlled category should not be tracked across websites or platforms without the user's consent and no functionality should be lost if a user determines they do not wish to be tracked.

The user-controlled category should still allow for business models that would offer users reduced monetary expenses, received payments, or like kind exchanges for their valuable personal data.

There are many ways to explore the concept of user-controlled data. Some activities that could be included, but not limited to this category, might be: search, browsing, and viewing/listening habits. The user-controlled category falls in between non-sensitive and sensitive user data. It is data that is not about the user, but about the user's aggregated habits. This type of data likely does not fall into the category of requiring breach notification, but the user should have a level of decision-making power over its collection, thus user controlled.

However, there is a difference between using live-time consumer data for the functionality of a service or device, versus tracking or storing data for other purposes outside the functioning of the device or particular product experience.

By using a website, App, or platform a user is sharing their data and habits with that company, and that company should be able to use data obtained within their own universe to enhance products and services, but once a user leaves that platform, they should be able to do so without being tracked.



For example, a Search Engine or Browser knows what was searched for and what link was clicked on, but it does not need to retain knowledge of how the user interacted with the page visited or how long the user was on the page.

To further illustrate, while using an Online Marketplace or Streaming Service, the Marketplace and/or Streaming Service has data on a user's shopping, viewing, and/or listening habits that are shared by virtue of using the service. The Marketplace or Streaming Service should be able to use that data to enhance user experience on the platform, for example product recommendations; however, when a user leaves the website, tracking should not continue without user consent.

To take the example a step further, if the user visited a Marketplace or Streaming Service through a Search Engine or Browser, the Search Engine or Browser should not be following all that the user is doing on other websites unless the user consented to such exchanges. This should also apply to the infrastructure these services operate through.

By using a service, operating system, software, or device a user is sharing their data and habits with that company, but the company should not be able to track the user within other services, operating systems, software, or devices that the initial implement allowed the user to access.

This concept is illustrated through the relationship between mobile devices and Apps. The act of using the device and operating system of the phone, should not equate to the relinquishment of all control over a user's data. When entering an App, the data should be confined to that App and not communicated with the operating system and used without consent.

While there is a difference between companies that sell products to users and companies that sell user data, the concept of user-controlled data does not need to be sector specific. **These ideas on user-controlled data translate to certain interactions taking place around the traditional business-customer relationship when there is a data exchange.** For example, data gathered via customer loyalty cards and apps, or through interaction with a device such as a motor vehicle or other machine that also collects/analyzes data.

I am happy to discuss these ideas further or answer any questions you may have.

Regards,

Katie McAuliffe
Executive Director
Digital Liberty



Internet Association

The unified voice of the internet economy / www.internetassociation.org

February 25, 2019

Chairwoman Jan Schakowsky and Ranking Member Cathy McMorris Rodgers
House Committee on Energy and Commerce
Rayburn House Office Building 2125
Washington, D.C. 20515

Dear Chairwoman Schakowsky and Ranking Member McMorris Rodgers:

Internet Association¹ (IA) welcomes the opportunity to submit this letter and our enclosed principles for a national privacy framework for the record as part of the Committee's February 26 hearing "*Protecting Consumer Privacy in the Era of Big Data*."

IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society and the economy and, as the voice of the world's leading internet companies, IA works to ensure legislators, consumers, and other stakeholders understand these benefits.

We 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.

IA released privacy principles in support of an American approach to federal privacy legislation that is consistent nationwide, proportional, flexible, and enables companies to act as good stewards of personal information provided to them by individuals. IA's proposed principles include:

- **Transparency.** Individuals should have the ability to know if and how personal information they provide is used and shared, who it's being shared with, and why it's being shared.
- **Controls.** Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, unless that information is legally required, or is necessary for the basic operation of the business.
- **Access.** Individuals should have reasonable access to the personal information they provide to companies. Personal information may be processed, aggregated, and analyzed to enable companies to provide services to individuals.
- **Correction.** Individuals should have the ability to correct the personal information they provide to companies, except where companies have a legitimate need or legal obligation to maintain it.
- **Deletion.** Individuals should have the ability to request the deletion of the personal information they provide to companies when it's no longer necessary to provide services, except where companies have a legitimate need or legal obligation to maintain it.

¹ Internet Association represents <https://internetassociation.org/our-members/>.



- **Portability.** Individuals should have the ability to take the personal information they have provided to one company and provide it to another company that provides a similar service.

IA's privacy principles place a heavy emphasis on context as the basis for any new national privacy framework. This means that such a framework must be flexible, taking into account the reasonable expectations individuals have regarding how the personal information they provide companies will be used, the sensitivity of personal information they provide to companies, and the concrete risk to individuals of the potential misuse or unanticipated sharing of such personal information. This risk-based approach will protect consumers when they need it most and also recognize that data—even the same piece of information—can present different harms based on who has it and how it is being used.

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.

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.

Sincerely,



Michael Beckerman
President and CEO

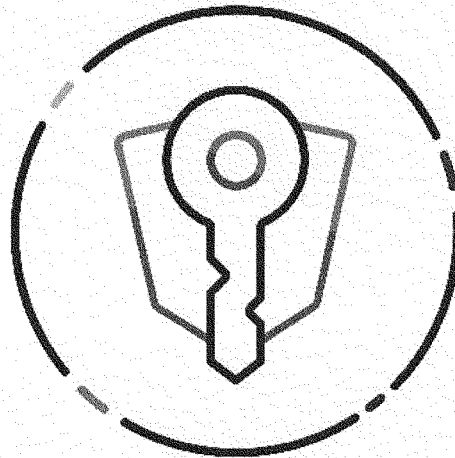


Internet Association

The unified voice of the internet economy / www.internetassociation.org



Internet Association



IA Privacy Principles For A Modern National Regulatory Framework

Internet Association

January 2014



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.² Additionally, there are myriad state laws relating to privacy and data security, enforced by

² These are the Children's Online Privacy Protection Act ("COPPA") and the FTC's COPPA Rule; the Gramm-Leach-Bliley Act, and the FTC's Privacy and Safeguards Rules; the Electronic Fund Transfer Act; the Fair Credit Reporting Act; the Fair and Accurate Credit Transactions Act; the Equal Credit Opportunity Act; The Truth in Lending Act; the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003 and the FTC's CAN-SPAN Rule; the Telephone Consumer



state attorneys general or private litigants, including state data breach notification statutes and unfair and deceptive acts and practices statutes; data security and encryption laws; and a variety of other privacy laws that relate to online privacy, social security numbers, and data brokers. Our member companies comply with these current laws as well as with self-regulatory principles and rules that govern how they operate and do business.³ However, this array of laws also creates a "patchwork" effect that complicate compliance efforts and lead to inconsistent experiences for individuals. A new, comprehensive national framework would create more consistent privacy protections that bolster consumers' privacy and ease compliance for companies.

This document sets forth: (1) principles for a national privacy framework, and (2) considerations for policymakers when evaluating such a national privacy framework.

Privacy Principles

These privacy principles aim to protect an individual's personal information, which we define as any information capable of identifying a specific individual or a device that belongs to that individual.

- **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.
- **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

Protection Act; the Restore Online Shopper's Confidence Act; the Video Privacy Protection Act; the Cable Act; the Electronic Communications Privacy Act; the Computer Fraud and Abuse Act; the Stored Communications Act; the Telemarketing and Consumer Fraud and Abuse Prevention Act and the FTC's Telemarketing Sales Rule, including the Do Not Call Rule and Registry; and the U.S. Safe Web Act.

³ These self-regulatory bodies have developed their own codes of conduct, including the Data and Marketing Associations Ethical Business Practices; the Network Advertising Initiative's 2018 Code of Conduct; the Digital Advertising Alliance's set of Self-Regulatory Principles relating to online advertising, which are enforced by the Accountability Program of the Council of Better Business Bureaus; and the Payment Security Industry Data Security Standards (PCI-DSS), for those that accept payment cards.



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.

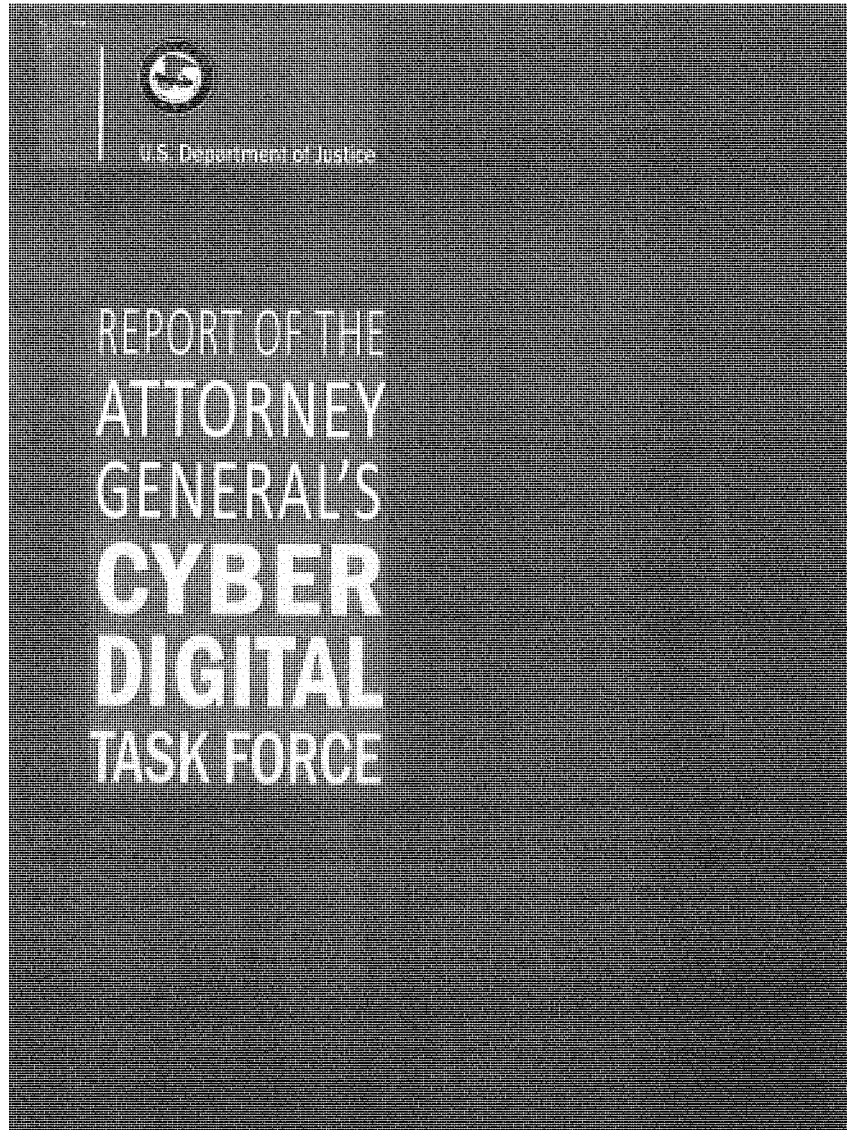


TABLE OF CONTENTS

LETTER FROM THE DEPUTY ATTORNEY GENERAL	i
ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE	vii
INTRODUCTION	xi
CHAPTER 1	
COUNTERING MALIGN FOREIGN INFLUENCE OPERATIONS	1
CHAPTER 2	
CATEGORIZING SOPHISTICATED CYBER SCHEMES	23
CHAPTER 3	
DETECTING, DETERRING, AND DISRUPTING CYBER THREATS	49
CHAPTER 4	
RESPONDING TO CYBER INCIDENTS	83
CHAPTER	
TRAINING AND MANAGING OUR WORKFORCE	95
CHAPTER 6	
LOOKING AHEAD	109
APPENDICES	
APPENDIX 1: MEMORANDUM ESTABLISHING THE TASK FORCE	131
APPENDIX 2: RECENT SUCCESSFUL BOTNET DISRUPTIONS	133
APPENDIX 3: RECENT SUCCESSFUL DARK WEB DISRUPTIONS	137
APPENDIX 4: GLOSSARY OF KEY TERMS	141

digital evidence on scene, subpoenas and search warrants can be obtained if the victim prefers. In either case, investigators are committed to working collaboratively with victims to minimize any disruption to business during an investigation.

After obtaining digital copies of any affected devices, investigators may then turn to other devices in the victim's architecture, including firewalls, log servers, and routers, to look for additional evidence of the perpetrator's presence. Investigators will also image these devices, as needed, and forensically examine them. Such devices often contain traces of a criminal's passage through the infrastructure on the way to the affected device. In particular, many devices maintain log files that show when, and from where, the device was accessed. In addition to preserving and copying digital evidence, investigators may interview employees (especially those tasked with responding to cyber threats or securing infrastructure), regular users of the affected systems, and management.

2. Online Data Review and Reconnaissance

After reviewing information obtained from a victim or other primary sources of information regarding a cyberattack, investigators frequently will review online data, which may be open source, to determine their next investigative steps. In undertaking these actions, as with all their actions, investigators are trained to act consistently with our Nation's rule of law principles, and with our society's foundational respect for civil rights and civil liberties.²

The first step in online reconnaissance often involves use of the Internet Corporation for Assigned Names and Numbers' WHOIS database.³ WHOIS is a directory of all of the IP addresses and domains on the Internet. WHOIS records usually display the name and contact information of the registrar (the business that sold the IP address or domain). Investigators can use the contact information to send legal process to the registrar in order to discover more information about the registrant (the user of the IP address or domain). WHOIS often contains self-reported information about the registrant, as well. In addition, an investigator often can tell from WHOIS and related information where a website is being hosted or who is hosting the e-mail server for a website, either (or both) of which can provide additional avenues for investigation.

After consulting WHOIS, investigators often perform online reconnaissance of the identifiers they have collected. This reconnaissance includes web searches looking for whether the identifiers have been used elsewhere and searches of social media to determine whether the identifiers are related to any accounts.

3. Searching Records from Online Providers

Successful WHOIS searches and online reconnaissance often results in the identification of e-mail providers, social media companies, registrars, and web hosting and computer hosting companies that may control additional evidence about a subject or

Protection Regulation (“GDPR”), which went into effect on May 25, 2018.

Broadly speaking, the GDPR regulates how private companies and governments process, store, and transfer data concerning E.U. residents, including how such data and information is handled and transferred into and out of the E.U. Violators could be subject to fines up to 4% of their gross revenue worldwide or 20 million Euros, whichever is greater, creating a serious financial incentive for covered entities not to violate the new regulation. Exceptions written into the GDPR should ensure that it does not affect the ability of U.S. law enforcement to obtain evidence through MLATs. Also, law enforcement-to-law enforcement sharing is covered by a separate directive and is thus outside of the scope of the GDPR. Still, significant questions and uncertainties exist about the GDPR, which could negatively affect law enforcement, including by impeding information sharing.

For example, some interpret the GDPR to require that the publicly-available WHOIS system remove information about the registrants of Internet domain names from public access, thereby necessitating the building and maintenance of secured law enforcement portals to access that information. As described in Chapter 3, prosecutors and law enforcement agencies around the world use the WHOIS system thousands of times a day to investigate crimes ranging from botnets to online fraud. The registrant data in WHOIS can create crucial leads to targets’ identities, locations, and other pieces of their criminal infrastructure. This data can also help identify additional victims. Due to the significant

risk associated with noncompliance with the GDPR, however, the private organization responsible for maintaining WHOIS has decided to remove much of the registrant data from the publicly-available segments of the system while the organization works with stakeholders, including the Department, to develop a GDPR-compliant system.

This is only one example of how the GDPR may be interpreted to impede the ability of law enforcement authorities to obtain data critical for their authorized criminal and civil law enforcement activities. Uncertainty about the GDPR also has placed in question not only voluntary disclosures of information about criminal activity—*e.g.*, by their employees, contractors, or customers—to U.S. law enforcement agencies, but also may cause companies with a significant E.U. presence to become reluctant to comply even with disclosures required by legal process, such as warrants and subpoenas, for fear that such a disclosure would be in violation of the GDPR. Absent official guidance, companies with significant E.U. business may become reluctant to participate in mandatory data transfers to U.S. law enforcement and regulatory authorities, which would impede effective tax collection, limit the ability of agencies to stop anti-competitive business practices, impair the work of public health and safety agencies, and undermine the integrity of global banking, securities, and commodities markets. This could also undercut the Department’s mitigation programs for businesses and individuals that wish to cooperate in areas such as fraud, bribery, money laundering, sanctions violations, and antitrust matters—programs that yield information



Google is pleased to provide comments to the House Committee on Energy and Commerce for the record of its hearing on “Protecting Consumer Privacy in the Era of Big Data.” This hearing and the committee’s ongoing work on privacy is both timely and important. We welcome the opportunity to contribute to the renewed discussion of how best to improve the U.S. regulatory framework for privacy.

Google believes the application of a comprehensive, balanced, risk- and outcomes-based framework that applies across economic sectors will improve privacy and security protections for individuals and communities and establish user trust while promoting continued societal and economic benefits made possible by the free flow and innovative uses of data.

Across every single economic sector, government function, and organizational mission, data and technology are critical keys to success. With advances in artificial intelligence and machine learning, data-based research and services will continue to drive economic development and social progress in the years to come, from agriculture and medicine to charitable and government services, and beyond. Businesses of all types and sizes collect and use data to drive efficiency, reduce costs, connect to markets, and improve the consumer experience.

At Google, we combine cutting-edge technology with data to build and improve the quality of products and services. These products help enhance people’s productivity, grow the economy,¹ improve accessibility,² make the web safer and more secure,³ and more. With partners, we are working to tackle big challenges⁴ and enable medical⁵ and scientific breakthroughs.⁶

For 20 years, our flagship products have been free, with advertising as our main source of revenue. We make the choice to build products for everyone, regardless of their economic circumstances, what connectivity they have, or what devices they use. By showing relevant, useful ads, we can deliver products like Search or Maps for free.

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

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

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

⁴ <http://refreshfoodandtech.com>

⁵ Working with physicians and other healthcare experts, we’ve developed systems that can detect diabetic eye disease (<https://ai.googleblog.com/2016/11/deep-learning-for-detection-of-diabetic.html>) and breast cancer tumors (<https://ai.googleblog.com/2018/02/assessing-cardiovascular-risk-factors.html>), help predict medical outcomes (<https://ai.googleblog.com/2018/05/deep-learning-for-electronic-health.html>), and even shed light on connections between cardiovascular disease and images of the eye (<https://ai.googleblog.com/2018/02/assessing-cardiovascular-risk-factors.html>).

⁶ We’ve shown machine learning can help predict molecular properties, which could aid everything from pharmaceuticals to photovoltaics to basic science (<https://ai.googleblog.com/2017/04/predicting-properties-of-molecules-with.html>). Another example is that Google’s AI technology helped discover the first 8-planet system outside our own solar system (<https://www.blog.google/technology/ai/hunting-planets-machine-learning/>).



Moreover, much of what we all enjoy online everyday — from free apps to independent media to services offered by small businesses — is supported by advertising.

All these benefits rely on the responsible collection and use of data, and must come with, and not at the expense of, privacy and security.

Toward A Comprehensive Baseline Privacy Framework

Google firmly believes that federal legislation is the best path to realize improved protections and reaffirms our long-standing support for smart and strong comprehensive baseline privacy legislation that enshrines high standards of privacy for everyone.⁷ Though there are meaningful and effective privacy protections in existing domestic law, regulations, and jurisprudence, we can improve upon the current framework with a comprehensive baseline privacy law that extend rights and protections by codifying long-standing privacy principles and unifying the U.S. approach. If well-crafted, the new baseline could make privacy more workable for all Americans and provide the certainty and flexibility businesses of all types and sizes depend upon to continue investing and innovating.

Moreover, digital trade has become an engine of economic growth for large and small businesses around the world, and the flow of data now contributes more to GDP growth than the flow of goods. A federal comprehensive baseline privacy law would help promote and sustain US global leadership around the free and open Internet, including promoting cross-border data flows and compatible pro-innovation rules globally.

In furtherance of those goals, we released a Framework for Responsible Data Protection.⁸ It provides the foundation of our comments.

Our framework is based on the Fair Information Practices Principles (FIPPs), OECD Privacy Principles, Asia-Pacific Economic Cooperation (APEC) Privacy Framework, aspects of the European General Data Protection Regulation (GDPR), and our 20 years of experience offering services that depend on information, privacy protections, and user trust, as well as our compliance experience. For example, over the last two years, we have engaged in a company-wide effort to prepare for the European Union's General Data Protection Regulation (GDPR), further improving on the robust information and tools we provide to users and on Google's industry-leading privacy program.

⁷ In comments to the Department of Commerce [Docket No. 101214614-0614-01 and Docket No. 1004] in 2010, Google called for the passage of comprehensive baseline privacy legislation.

⁸ https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf



Individual-Centric Privacy Outcomes

At its core, comprehensive baseline federal legislation should be consistent, adaptable, and proportional, and implemented in a manner that provides individuals with a meaningful ability to control and to obtain information about and access to their data, while protecting the privacy of others and providing a practicable framework for compliance. Legislation should focus on transparency; control; responsible and reasonable data collection and use; security; access, correction, portability, and deletion; and accountability.

Transparency

All organizations that collect and use personal data should be required to provide notice about the types of personal information they collect, why they collect it, and how they use and/or disclose it, particularly when used to make decisions about the individual. Making this information available is critical to building and maintaining user trust.

Privacy policies provide a comprehensive source of this information for individuals, regulators, and experts to more systematically review the organization's data collection and processing practices, and hold them accountable for the representations they make. Given the array of issues and services these policies need to address, they can be long and difficult to parse, turning off many individuals from reading them. A key challenge for organizations is how to provide individuals necessary information without extraneous details or difficult text that can be overwhelming.

At Google, we regularly refine our approach based on continuous research and feedback from our users to ensure we strike this balance effectively. Though our privacy policy has long been recognized as best in class,⁹ we recently updated it to incorporate some of the insights we have gained and make it more understandable and accessible to users, regardless of how much time they spend to review it, while being a full and complete statement of our data practices. We simplified our language and incorporated clear headings, easier navigation, overlays and examples, explanatory videos, and in-line settings so users can make decisions about their account settings as they learn about our practices.

Regulators should encourage organizations to go beyond the privacy policy and actively inform individuals about data use in the context of the services themselves, helping to make the information relevant and actionable for individuals. For example, if you add a Google Drive file to a shared folder, we will check to make sure you intend to share that file with everyone who has access to that folder. With Why This Ad,¹⁰ you are

⁹ Time Magazine and the Center for Plain Language ranked Google number one among technology companies for best privacy policy (<http://time.com/3986016/google-facebook-twitter-privacy-policies/>).

¹⁰ <https://support.google.com/ads/answer/1634057?hl=en>



able to click or tap on an icon in or around each ad to find out why you are seeing that particular ad and understand more about how Google's ad system makes these decisions.

In addition to our efforts on transparency mentioned above, recently we improved transparency and user control in our flagship product, Search, with a tool that shows users exactly how their data is being used to improve their search results, along with direct access to controls.¹¹

Finally, our Transparency Report¹² provides information to the public on how government actions can affect the free flow of information online. We are always working to expand the information we provide to users.

Control

People have different preferences about how they want their information to be used, and preferences can vary over time. A regulatory framework should not presume all individuals are the same and should ensure it is practical for individuals to control the use of personal information, no matter what entity is collecting or processing it.

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

We support the GDPR's notion of "legitimate interests" as a meaningful way to permit standard or typical data uses that are consistent with individuals' interests while reserving express consent to those situations where individuals need to pause and consider their choice. The specifics of consent (e.g., what options should exist and how they are presented) should not be enshrined in statutory language but articulated in regulatory guidance and codes of conduct that can be updated as norms and technology changes. This will be particularly important as emerging technologies become more widespread, such as screenless devices and ambient computing systems.

Dashboards are a recognized best practice to make individual controls easy to find and practical to use, and we think should be broadly implemented.¹³ Google was one of the first companies to offer users a centralized dashboard in 2009. Users who have a

¹¹ <https://www.blog.google/technology/safety-security/making-it-easier-control-your-data-directly-google-products/>

¹² <https://transparencyreport.google.com/?hl=en>

¹³ Dashboards are a recognized best practice (<https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf>).



Google account can find their privacy and security settings in a single place - Google Account¹⁴ - and need not visit several different apps or pages to access their data and set their preferences for how Google should use their information. Google Account is where users are able to download a copy of their personal information; access or delete their Google activity (such as search queries or browsing history) by date, product, or topic; disable personalized ads or see the information Google uses to personalize their ads; and locate a lost or stolen phone.

One part of the Google Account is the Google Security Checkup¹⁵ and Privacy Checkup¹⁶ tools, which help users identify and control the apps that have access to their Google account data, and guide users to review and change their security and privacy settings. We regularly and actively prompt users to do privacy and security reviews by reminding them to use these tools through individual prompts and service-wide promotions.

We continue to develop and improve these and other tools to make them more robust and intuitive, and these efforts are working: nearly 2 billion people visit their Google Account controls and more than 100 million people take a Privacy Checkup each year.¹⁷

Responsible and Reasonable Data Collection and Use

Comprehensive baseline privacy legislation should require organizations to operate with respect for individuals' interests when they process personal information. Organizations must also take responsibility for using data in a way that provides value to individuals and society and minimizes the risk of harm based on the use of personal information, such as data that can be linked to a specific person or personal device.

A key part of the responsible collection and use of data is reasonable data minimization obligations. We believe a regulatory framework should place reasonable limitations on the manner and means of collecting, using, and disclosing personal information. Reasonable data minimization obligations should be scoped as to not discourage data collection and use, so long as that collection and use is deliberate and thoughtful, in a manner compatible with individuals' interests and societal benefits, and circumscribed and in accordance with the organization's privacy program and regulatory guidelines. At the same time, it should discourage collection and use of more identifying information if less identifying information (e.g., pseudonymous or de-identified data) is sufficient.

¹⁴ <https://myaccount.google.com/intro?hl=en-US>

¹⁵ <https://myaccount.google.com/security-checkup>

¹⁶ <https://myaccount.google.com/privacycheckup?otzr=1>

¹⁷ See: <https://www.blog.google/technology/safety-security/improving-our-privacy-controls-new-google-dashboard/>, <https://www.blog.google/technology/safety-security/celebrating-my-accounts-first-birthday/>, and <https://googleblog.blogspot.com/2015/06/privacy-security-tools-improvements.html> for more information.



Another component of responsible and reasonable data collection and use is data quality. Comprehensive baseline privacy legislation should ensure organizations make reasonable efforts to keep personal information accurate, complete, and up-to-date to the extent relevant for the purposes for which it is maintained. Data access and correction tools, as mentioned below, can assist organizations in meeting this obligation.

Security

Organizations must implement reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, modification, and destruction. Baseline precautions should apply to any collection of personal information, and additional measures should account for the sensitivity of the underlying information and be proportionate to the risk of harm.

As a corollary, organizations should be required to expeditiously notify individuals of security breaches that create a significant risk of harm. Google has long supported legislation that would establish a national security breach notification regime. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have adopted security breach notification laws. While these laws share the common aim of protecting individuals in the aftermath of a security breach, they vary in specifying the manner in which individuals must be notified, the content of security breach notifications, and the regulatory entities that must be notified, among other things. A national security breach notification standard can simplify the notification process itself while ensuring that individuals are empowered to take measures that can reduce the likelihood of identity theft, fraud, or other types of harms. We encourage Congress to incorporate a national security breach notification standard as a component of new legislation.

Access, Correction, Portability, and Deletion

Privacy law should also ensure individuals, where practical, have the ability to access, correct, delete, and download and export personal information. This not only empowers individuals, it also keeps the market innovative, competitive, and open to new entrants.

Google strongly supports the notion that users should be able to export the personal information they have provided to an organization in a format that allows them to understand the information, store a local copy, download it and/or to import it into another provider's systems. We believe this is critical to include in any privacy framework, but note data portability is not, and should not be, absolute. Portability efforts should be limited to content an individual user creates, imports, or has control over and should not include data companies generate that may be commercially



sensitive or proprietary. Along with access mechanisms, it should also be limited to individuals a covered entity is able to authenticate.

Google has worked on portability for over a decade and was the first to offer a portability tool in 2011. We recently updated and broadened this tool, Download Your Data, so that it now covers more products and data types. The tool allows users to take personal information about them stored in more than 50 Google products, including search queries, Gmail messages and contacts, YouTube videos, and many others. The output is provided in formats designed to be importable into software on the user's own devices or other services.

The ability for users to transfer data directly from one provider to another, without downloading and re-uploading it, is a significant advancement in making portability practical for users all over the world. However, service-to-service portability remains nascent, thus it should not be a requirement or included in control or other privacy obligations.

We are working with partner companies on the Data Transfer Project,¹⁸ an open-source initiative to expand this capability and make it even easier for users to try a new service or otherwise control their data. The current partners (Google, Microsoft, Twitter, and Facebook) are working on building a user interface as well as bringing new and more diverse partners into the project. We will continue to encourage more partners to join our efforts and facilitate broader availability of service-to-service portability.

We urge Congress to explore ways to develop data portability that works for businesses of all types and sizes. One way to further this goal is for industry organizations and government entities like the Federal Trade Commission to explore best practices and methodologies that can be adopted by smaller organizations — perhaps via open-source projects or other low-cost options.

Accountability

A privacy regulatory framework should be principles-based and prioritize outcomes over means. When put in practice, goals and outcomes are often conflated, leading to one-size-fits all rules. To achieve both legal certainty and flexibility, Congress should set clear baseline requirements and enable organizations to decide how to meet those requirements.

Accountability can and should come in many forms. For example, industry accountability programs and safe harbors can incentivize best practices, particularly in providing more flexible approaches to dealing with evolving technologies. Also, companies should be encouraged to create accountability through internal privacy programs that, among other things, build in privacy from the ground up for product

¹⁸ <https://datatransferproject.dev>



development. At the same time, we believe the establishment of internal programs should be scalable: small businesses can achieve the same protections and accountability without building a privacy program with the same scope and scale that larger, more established companies like Google operate.

In considering accountability, it is important to keep in mind the distinction between consumer services and enterprise services, and the need to clarify obligations based on an organization's ability to meet those obligations. Much processing of personal information is done by one company on behalf of another, where the service provider or "processor" lacks legal authority to make independent decisions about how to use the data or operate outside the bounds of the client's direction. Sometimes this distinction is described as "processors" versus "controllers", allowing for the efficient use of vetted, qualified vendors with minimal additional compliance costs, which is particularly important for smaller entities. Controllers remain responsible for meeting certain obligations under the law, including transparency, control, and access, but processors must still meet basic programmatic and security responsibilities.

Goals for Federal Legislation

We agree that high-level goals for federal action are important and should be considered separately from privacy outcomes. In the following section, we provide further information on what we suggest Congress consider as it further develops its approach and how these goals might be achieved.

Create a Unified Approach.

Privacy law should regulate organizations to the extent they are active within the jurisdiction. Extra-territorial application does not align with established territoriality principles, unnecessarily hampers the growth of new businesses, and creates conflicts of law between jurisdictions. In particular, we believe that small and medium-sized businesses shouldn't have to worry about running afoul of regulators in different jurisdictions merely because a few people from another state or country navigate to their website or use their service.

Design Regulations to Improve the Entire Ecosystem and Accommodate Changes in Technology and Norms.

The technology involved in data processing is not static, and neither are the social norms about what is considered private and how data should be protected. A baseline law can provide clarity, while ongoing reviews (e.g., regulatory guidance, codes of conduct, administrative hearings) can provide more flexible and detailed guidance that can be updated without wholesale restructuring of the legal framework. The U.S. Government can support these goals by rewarding research, best practices, and



open-source frameworks. Creating incentives for organizations to advance the state of the art in privacy protection promotes responsible data collection and use.

Comprehensive Application

User-centric privacy outcomes will also come from neutral, comprehensive, and consistent application of privacy rights and obligations. Data is increasingly important through all sectors of the modern economy, and generally individuals neither want nor expect different baseline privacy rules based on the provider collecting and using their personal information, the type of service they use, or where they live. At the same time, organizations are increasingly competing across sectors, and a regulatory regime should apply in a manner neutral to industry, technology, and business model.

Congress should both take care to avoid unnecessary distinctions between industries or business models. We strongly believe that aside from the context of particular relationships that have existing rules, like with one's employer or attorney, legislation should apply to all economic sectors and all types of organizations that process personal information. While certain sectors (e.g., healthcare) may have additional rules, regulation should set a baseline for all organizations.

The application of the law should also take into account the resource constraints of different organizations, encouraging, rather than stymieing, new entrants and diverse and innovative approaches to compliance. One way to further this goal is for industry organizations, government entities, and civil society organizations to share best practices, methodologies, lessons learned, and techniques that can be adopted, particularly by smaller players. All organizations can and should innovate as much on protecting privacy and security and enabling individual control as they do on products and services.

Focus on Risk of Harm

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

Encourage Regulatory Compatibility and Cross-Border Data Flows.

Mechanisms allowing for cross-border data flows are critical to the modern economy. Organizations benefit from consistent compliance programs based on widely shared principles of data protection. We encourage Congress to adopt a globally integrated framework, and avoid conflicting and unpredictable requirements, which lead to



inefficiency and balkanization of services and create confusion in consumer expectations. Privacy regulation should support cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms that ensure protections follow the data, not national boundaries.

Some countries have taken steps to limit cross-border data flows through forced data localization requirements. Such requirements fail to recognize the way that modern distributed networks function and could have the unintended consequence of weakening privacy and security protections.¹⁹ A comprehensive federal data protection law that explicitly eschews data localization would serve as a bulwark against data localization requirements and lend credence to the idea that countries can protect privacy on a cross-border basis without compromising key digital trade principles. A federal law could also build on recent steps taken by the US, Mexico, and Canada in the United States-Mexico-Canada Agreement (USMCA) to require protection of the personal information of users of digital trade and to promote compatibility between different privacy frameworks. It is important to promote a regulatory landscape that is consistent with international frameworks for protecting privacy, including the APEC Cross-Border Privacy Rules System.

Incentivize Research and Development

Google is grateful to have a close relationship with the privacy and security research community, and maintains a permanent privacy and security research team that is dedicated full time to researching privacy and security issues. This research serves both to inform the teams building products about important privacy and security issues, as well as to engage and contribute to the vibrant research community, and is frequently published and presented in external journals and conferences. These teams also engage directly with users through user experience studies, to ensure that our products and policies are built with users in mind and based on their feedback.

Though organizations like Google invest significantly in research and development, Google believes the federal government has a critical role in enabling advancement of privacy and security enhancing technologies, techniques, and approaches.

We encourage the federal government to continue providing funding for the research and development of products, services, and techniques that improve privacy and security protection. Basic research remains cost intensive, and educational institutions and research organizations need sustained funding to make the critical long-term investments that lead to new and improved ways to protect privacy and security. However, in its support, the government should not only focus only on the products and services that individuals see as an end-result, but also on expanding the types of tools and training available to practitioners. For example, techniques for internal data

¹⁹ <https://www.blog.google/products/google-cloud/freedom-data-movement-cloud-era/>



management and expanded availability of ethics and interdisciplinary training in schools and other educational contexts can promote better outcomes for individuals.

The federal government should also consider establishing local centers of excellence for privacy and security research and applications, perform privacy and security research at government labs and agencies, create frameworks and mechanisms to facilitate public-private sector collaboration, and explore incentives for researchers who receive public funding to explore priority research areas. Google has long supported open-source research, and we encourage open access to publicly funded research.

Lastly, the federal government should leverage its convening power to disseminate best practices and effective tools and approaches to ensure that every organization that processes personal data, including the government itself, can keep abreast of and implement the state of the art. Publications, public events, technical workshops, digital literacy programs, and advisory committees, are potential ways it could achieve this goal.

Defining Key Terms

Finally, the definitions that establish the foundation of any legal privacy framework are essential to scope appropriately. Personal information should be defined flexibly to ensure appropriate incentives and handling. The scope of legislation should be broad enough to cover all information used to identify a specific user or personal device over time and data connected to those identifiers, while encouraging the use of less-identifying and less risky data where suitable. The law should clarify whether and how each provision should apply, including whether it applies to aggregated information, de-identified information, pseudonymous information or identified information.

In crafting privacy regulation, the federal approach should be closely bound to an articulation of risk of harm. For example, Google's Framework for Responsible Data Protection Regulation suggests that "sensitivity" of personal information should be tied in law to risk of harm to individuals and communities, rather than a specific list of data types that might quickly become out of date. We think this is the right approach, but does require thought to avoid unnecessarily shifting regulatory standards.

Conclusion



As Congress considers potential comprehensive baseline privacy legislation, we recommend consideration of the importance of responsible data practices for consumers, the impact of a regulatory framework on service functionality, the consumer benefits of free and low-cost products, the future of the open web and app ecosystem, and the unique compliance needs of small businesses to ensure smart and strong regulations that mitigate undesired tradeoffs.

Thank you again for this opportunity to provide comments. Google appreciates the opportunity to share its perspective and experience. We are happy to answer questions or provide further information with respect to privacy and Congress's work to develop a regulatory framework.

Respectfully submitted,

Google



317.875.5260 | F: 317.879.8408
 3601 Vincennes Road, Indianapolis, Indiana 46268
 202.628.1558 | F: 202.628.1601
 20 F Street N.W., Suite 510 | Washington, D.C. 20001

February 26, 2019

The Honorable Frank Pallone
 2107 Rayburn House Office Building
 Washington, DC 20515

The Honorable Janice Schakowsky
 2367 Rayburn House Office Building
 Washington, DC 20515

The Honorable Greg Walden
 2185 Rayburn House Office Building
 Washington, DC 20515

The Honorable Cathy McMorris Rodgers
 1035 Longworth House Office Building
 Washington, DC 20515

Dear Representatives:

On behalf of the National Association of Mutual Insurance Companies (NAMIC), I write regarding the Subcommittee on Consumer Protection and Commerce hearing on "Protecting Consumer Privacy in the Era of Big Data" on February 26, 2019. NAMIC has been a leader in the property/casualty insurance industry in the conversation surrounding data security and privacy and we appreciate your committee's focus on such a crucial issue of national importance.

NAMIC is the oldest property/casualty insurance trade association in the country, with more than 1,400-member companies representing 41 percent of the total market. NAMIC supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC member companies serve more than 170 million policyholders and write more than \$253 billion in annual premiums. Our members account for 54 percent of homeowners, 43 percent of automobile, and 35 percent of the business insurance markets. Through our advocacy programs, we promote public policy solutions that benefit NAMIC member companies and the policyholders they serve and foster greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

We are writing to the Committee to express our support for uniformity across the country for data security and privacy standards for insurance companies. Any plan must provide for the recognition of unique industries such as the property/casualty insurance industry. The insurance industry currently faces a complex web of differing state requirements on breach notification and increasingly in data security standards. These inconsistencies force some in the insurance industry to wastefully focus on complying with differing standards instead of concentrating exclusively on protecting consumers' data.

We represent a wide assortment of companies providing valuable services to consumers, and any legislation should account for the different threats these entities face. Therefore, data security requirements should be risk-based and scalable; this



flexibility will ensure that companies have the necessary protections in place to secure consumer data proportionate with its risk and the evolving threat landscape.

Property/Casualty insurers, as you know, are functionally regulated by state insurance commissioners in all 50 states. These regulators bring considerable expertise and regional experience that surpasses the ability of the Federal government in the complex world of insurance regulation. We look forward to working with you to alleviate the problems caused by the patchwork of data security and privacy laws in a way that also reinforces the state-based regulatory framework that works well for insurers and policyholders.

As an industry that has extensive experience with data security and privacy compliance, we look forward to working with the Committee on this important issue. Thank you for your consideration and we would welcome the opportunity to discuss further.

Sincerely,



Jimi Grande
Senior Vice President, Government Affairs
National Association of Mutual Insurance Companies



**United States House Committee on Energy and Commerce
Subcommittee on Consumer Protection and Commerce
2125 Rayburn House Office Building**

March 15, 2019

To the Honorable Robin L. Kelly:

Please find the below response regarding the following question:

Many proposals direct the FTC to establish rules to address advertising practices that result in discrimination. Do you have ideas in mind for what kind of rules the FTC could put in place?

The FTC, or a newly created, well funded, and independent Data Protection Agency (DPA), empowered with full rulemaking authority, should rule that it is unlawful to process personal information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for housing, employment, credit, insurance, voting, or education opportunities, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of a person or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.

The FTC or DPA should promulgate regulations to define and prohibit unfair or deceptive advertising, targeting, personalization, and delivery practices. In specifying unfair or deceptive practices, the FTC or DPA should consider:

- Established public policy, such as civil rights laws, that can guide the determinations of what constitutes an unfair or deceptive practice;
- The methods available or used to target, personalize, and deliver online advertisements, and their effects;
- Research of, and methodologies for, measuring discrimination, including disparate impact, in advertising, targeting, personalization, and delivery practices;
- The role of all actors in the digital advertising ecosystem, including advertisers; social media platforms; search engines; websites and applications that carry advertisements; advertising networks; data brokers; personal device manufacturers; and other relevant entities;
- Harms caused by predatory or manipulative marketing practices targeting marginalized or vulnerable populations, including on the actual or perceived basis of race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial



status, biometric information, personal health information, lawful source of income, disability, age, criminal record, or immigration status;

- Whether, and at what age, minors are able to distinguish between regular content and paid advertisements;
- Methods for fairly promoting equal opportunity in housing, employment, credit, insurance, education, or healthcare, through targeted outreach to underrepresented populations in a fair and non-predatory manner;
- How to increase diversity and inclusion by fairly promoting content generated by and small businesses owned by members of underrepresented populations; and
- Other privacy risks posed by advertising, targeting, personalization, and delivery practices.

Crucially, any anti-discrimination provisions must allow actors to further equal opportunity in housing, education, voting, and employment by targeting underrepresented populations where consistent with civil rights laws.

Robust enforcement of the prohibition on discrimination should include both intentional efforts to discriminate as well as disparate impacts. To ensure robust enforcement and relief for those impacted, the FTC should also eliminate “first bite of the apple” under Section 5(m)(1)(B) which restricts the Commission’s ability to subject violators to monetary penalties. Additionally, a private right of action should be a part of these rules. Any person may bring an action seeking relief from a violation of the rules or regulations promulgated on their own behalf or on behalf of themselves and the general public. A nonprofit organization may also, on behalf of itself or any of its members, on behalf of an individual or class of individuals, or on any such behalf and on behalf of the general public, bring an action seeking relief from a violation of these rules

To ensure that discriminatory practices are monitored and addressed, the rules set forth by the FTC or DPA should require covered entities that are not small businesses to regularly audit their processes to determine that their practices work as intended and do not discriminate in a prohibited manner, and that they identify and implement reasonable measures to mitigate those discriminatory impacts.

I’m happy to say more or provide further information upon request.

Sincerely,

Brandi Collins-Dexter
Color Of Change



Questions for the Record before the House Committee on Energy and Commerce
Subcommittee on Consumer Protection and Commerce
On Protecting Consumer Privacy in the Era of Big Data

How the US Can Leapfrog the EU

The Role of Technology and Education in Online Privacy

Roslyn Layton
Visiting Scholar

March 27, 2019

The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the author.

Chair Schakowsky, Ranking Member McMorris Rodgers, and Members of the Committee, thank you for the opportunity to provide additional testimony for the record. Please find my answers to your questions. For ease of reading, the answers to the questions are organized by the respective Committee member.

Contents

Congresswoman Robin L. Kelly	2
Congresswoman Anna G. Eshoo	4
The Honorable Michael C. Burgess, M.D.	12
The Honorable Richard Hudson	19

Congresswoman Robin L. Kelly

1. Many proposals direct the FTC to establish rules to address advertising practices that result in discrimination. Do you have ideas in mind for what kind of rules the FTC could put in place?

Answer:

The Federal Trade Commission (FTC) has made a detailed report on this issue.¹ There are a formidable set of laws already which protect against harmful discrimination in advertising. The report notes how the Fair Credit Reporting Act and Equal Opportunity Laws protect against discrimination in advertising. Indeed, there is a risk that regulation which reduces the amount of information for decision making could create worse outcomes by increasing prices across the board to compensate for inaccuracies. This adverse outcome was found in a study of home loans in the San Francisco Bay Area in which counties which had the strictest privacy settings ended up paying more for mortgages and defaulting at a higher rate because the banks could not accurately match the applicant to the appropriate loan.²

Rather than restrict firms in their ability to use data, the FTC and other policymakers should

¹ <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

² Jin-Hyuk Kim & Liad Wagman, Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis, 46 RAND J. OF ECON. 1 (2015). This is consistent with the more general phenomenon of risk-based lending markets. See Wendy Edelberg, Risk-Based Pricing of Interest Rates for Consumer Loans, 53 J. MONETARY ECON. 2283 (2006)

encourage firms to improve the accuracy of their tools. Additionally, the effort should be bolstered with improving the readability of disclosures on business practices and consumer education about how online platforms work (discussed in another QFR), so that consumers can make better decisions about the online platforms they use.

Importantly the FTC report notes the importance of harnessing data practices for the betterment of the disadvantaged.

Businesses have strong incentives to seek accurate information about consumers, whatever the tool. Indeed, businesses use big data specifically to increase accuracy. Our competition expertise tells us that if one company draws incorrect conclusions and misses opportunities, competitors with better analysis will strive to fill the gap. . . Therefore, to the extent that companies today misunderstand members of low-income, disadvantaged, or vulnerable populations, big data analytics combined with a competitive market may well resolve these misunderstandings rather than perpetuate them. In particular, a company's failure to communicate premium offers to eligible consumers presents a prime business opportunity for a competitor with a better algorithm. To understand the benefits and risks of tools like big data analytics, we must also consider the powerful forces of economics and free-market competition. If we give undue credence to hypothetical harms, we risk distracting ourselves from genuine harms and discouraging the development of the very tools that promise new benefits to low income, disadvantaged, and vulnerable individuals.³

Improving the FTC's enforcement capabilities overall, notably with removing common carrier and non-profit exemptions, increasing the FTC's budget and headcount for online privacy investigations and enforcement, and allowing the FTC to levy civil penalties, would be helpful on this issue.

³ Supra FTC

Congresswoman Anna G. Eshoo

1. On June 28, 2018, then-Governor Jerry Brown signed into law A.B. 375, the California Consumer Privacy Act of 2018 (CCPA). A.B. 375 was first introduced by Assembly Member Ed Chau in 2017. A significant portion of the final law was adapted from a ballot initiative that was based on two years of research and was first submitted to the Attorney General of California in 2017.

During the hearing you stated that the CCPA is “a law that came together in one week.” For the record, please substantiate this statement.

Answer:

A.B. 375 was a highly flawed bill which attempted to reinstate the Federal Communication Commission’s ISP-only privacy rules, following their rejection under the Congressional Review Act.⁴ The FCC never conducted an assessment of the broadband providers’ privacy which would suggest that Federal Trade Commission’s rules were not working nor did it have a record of complaints that ISPs had violated consumers’ privacy. Indeed, the only reason that the FCC invented these rules was that the classification of broadband under Title II triggered the common carrier exemption, negating the FTC’s jurisdiction. The FCC’s move was reckless, as it left consumers with no privacy protections, and it enshrined a regulatory asymmetry in creating two different standards for online privacy, something which is confusing and opaque for consumers. Moreover, it created a de facto market entry barrier to the oligopoly advertising market dominated by a handful of California based platforms.⁵ Fortunately, the bill was withdrawn, but it likely violated the Constitution.⁶

The claim regarding the one-week deliberation is noted by Santa Clara University Law Professor. It was reiterated by more than 40 California based privacy professionals and lawyers. See Goldman, Eric, An Introduction to the California Consumer Privacy Act (CCPA) (July 9, 2018).

⁴ <https://www.forbes.com/sites/roslynlayton/2018/08/20/californias-internet-policy-may-have-good-intentions-but-is-it-progressive/#563247d2f450>

⁵ <http://www.aei.org/publication/fcc-privacy-regulation-will-limit-competition-market-really-needs-online-advertising/>

⁶ <http://www.aei.org/publication/californias-privacy-proposal-failed-but-it-probably-violated-the-constitution-anyway/>

Santa Clara Univ. Legal Studies Research Paper. Available at SSRN: <https://ssrn.com/abstract=3211013> or <http://dx.doi.org/10.2139/ssrn.3211013>

The view that the CCPA was hastily pasted together is also the Senate testimony of Evan Engstrom, Executive Director, Engine Advocacy and Research Foundation in San Francisco. He noted to the Senate Commerce Committee,

While CCPA's objectives are laudable, the process leading to its passage was not. Although the ballot initiative's authors clearly spent considerable time on their proposal, the legislature spent less than a week translating the initiative's general ideas into actual bill text. As a result, California legislators were unable to fully evaluate the bill, its impact on California's startup community, or its actual value to consumers. This rushed process resulted in a well-intentioned law that is full of typos, contradictions, security loopholes, and vague obligations.⁷

Engine detailed further concerns about the CCPA threatens startups with the California Attorney General and the Senate including but not limited to

1. The overly broad definition of personal information that does not explicitly exclude de-identified and aggregated data
2. The CCPA defines "sale" expansively, covering many commonplace practices that businesses rely on to provide goods and services to consumers.
3. The prohibition on differing service based on consumer privacy choices. In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups.
4. Privacy and security problems with CCPA's right to access and delete which create opportunities for fraud or needless requirements for additional data collection.
5. The private right of action creates uncertainty for startups. No matter how thorough a company's data security practice safe, determining whether they were legally "reasonable" is not amenable to early adjudication in a lawsuit.
6. CCPA's small business exemption fails to capture startups.
7. The design and procedure of the opt-out function does not sync with startups practices
8. The CCPA imposes significant compliance burdens for the diverse business models represented in California's startup ecosystem.⁸

⁷ https://www.commerce.senate.gov/public/_cache/files/949f1fc8-dc28-4760-9f47-6cb925a1549e/0AE3566F5899E50A6C4D08C7142D8752.testimony-of-evan-engstrom-engine.pdf

⁸

Give that internet startups are the lifeblood of Silicon Valley, these concerns about the CCPA should be addressed.

2. As we learned in the recent investigations of Motherboard and the New York Times, wireless carriers and apps are selling users' location data to hedge funds, bail bondsmen, bounty hunters, and stalkers. It's likely that your personal location data and mine are also being sold without our knowledge or consent. While some companies admit they sell user data, that information is usually buried deep in 10,000-word privacy policies that are hard to find and even harder to understand.

How, exactly, would transparency and consumer education, which you stress in your testimony as central to privacy legislation, solve the problem of data being used in egregious ways, even when companies disclose such practices?

Answer:

Following is a discussion of how to create policy with realistic conceptions of consumers, their different needs and capabilities, as well as how education and transparency can complement online privacy legislation. I do not suggest that education and transparency by themselves are sufficient or are substitutes for comprehensive federal privacy legislation (while they could be for some consumers), but I wish to underscore the point that consumers are not monolithic. They can learn, evolve, and change behavior. This is important to recognize in conceptualizing any regulation on the disclosure of data practices.

The current policy process on consumer privacy has been open and inclusive, surfacing the views of many stakeholders. While there is a understanding of different kinds of firms and organizations which collect data (large Silicon Valley platforms, Fortune 1000 firms, data brokers, small and medium-sized internet companies, public sector agencies, startups, non-profit organizations, individual blogs, websites etc.), the people who use these digital products and services are lumped into single box such as "consumers" or "users". Nevertheless, consumers have multiple parameters by which they can be described including age, gender, race, occupation, education, location, affiliation and so on.

Conceptualizing consumers as a monolithic group as if they all want the same regulation is wrong. This presumption can lead to misguided policy which ultimately fails to achieve its

<https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5c87c83c6e9a7f38beb04d5c/1552402492673/Engine+-+CCPA+comments.pdf>

stated goals, or to which firms and consumers find workarounds. Users of online services are highly diverse, have different preferences, and make individual, contextualized decisions based upon how they perceive the transaction with their data. Research tools deployed among hundreds of millions of users shows that privacy preferences change minute to minute depending on the site visited, the user's goal, and the user's desire for security and speed.⁹ Users interpret privacy within a context, and many don't object to sharing information per se, only to sharing that is inappropriate based on the context.¹⁰

While there is a benefit to a single, comprehensive standard, policymakers should realize that not all "consumers" are the same. The point is underscored by a leading data broker's categorization of consumers by "lifestage", affluence, and use of digital technologies.¹¹ American households are further categorized into 70 segments and 21 groups based on similar demographic, socio-economic and consumer behavior.¹² Hispanic consumers can be categorized into 55 specific buying groups.¹³ Understandably some regulatory advocates are opposed to such tools, even though they have been integrated in the American economy for decades, and prior to that, were conducted via analog means.

The point is merely that a data broker's description of "consumers" is a more accurate reflection than the current policy discourse. As such, it is worthwhile for policymakers to try to understand the diversity of consumers before making policy. Consumer education plays an important role to fill the gap between what regulatory advocates want and what different consumers prefer. As such, it makes sense to propose a baseline set of principles and to allow consumers to supplement their preferences with informed choices.

Responsibilities of consumers. The leading textbook of the field "Economic Education for Consumers" details the notions of consumer expectations as well as consumer responsibilities.¹⁴ They include the following concepts:

1. Responsibility to be an educated consumer, including responsibility to gather and evaluate information before making a decision

⁹ Scott Meyer, "The Next \$50 Billion Will Come From . . . Putting Users First," Ghostery Inc., <https://www.slideshare.net/ghosterybrand/the-next-50-billion-will-come-fromputting-users-first>.

¹⁰ HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2009), <https://www.sup.org/books/title/?id=8862>.

¹¹ "Acxiom Personix," accessed November 9, 2018, <http://www.personix.co.uk/personix.html>.

¹² "Consumer and Household Segmentation | Personix," Acxiom, accessed November 9, 2018, <https://www.acxiom.com/what-we-do/consumer-segmentation-personix/>.

¹³ *Ibid*

¹⁴ Roger LeRoy Miller and Alan D. Stafford, *Economic Education for Consumers* (Cengage Learning, 2009). p. 88

2. Responsibility to use products and services safely
3. Responsibility to use information to make choices
4. Responsibility to choose carefully
5. Responsibility to express opinion about a product, as well as report improper business practices. This can be communicated to the community, firm, and/or authorities.

In addition, consumers have the freedom to consume in a responsible manner by selecting products and services that conform to their values as well as seek redress from injury by unfair, deceptive, and defective products and services.

Role of Consumer Education in Online Privacy. Consumer education is by no means a panacea. Indeed an academic review of the range of methods and approaches employed for financial literacy education notes shortcomings in their effectiveness.¹⁵ On the other hand, the value of education to improve outcomes in personal health is well-documented.¹⁶ However financial literacy may be more effective in imparting “rules of thumb”, for example, knowing the value of diversification in an investment portfolio is more important than knowing the litany of financial instruments.¹⁷

It is instructive to consider the robust, vibrant market for information and education in the consumer electronics field detailing the most minute and technical aspect of machines. For decades consumers have availed themselves to magazines, online discussions, rankings, reviews, how-to videos, conferences, and so on. There is no policymaker directing the discussion, but it grows by consumer demand.

There is no reason why there could not be a similar field for the consumption of online services, which describes the contours of online privacy and how users could select different technologies to manage their privacy. The difference is that consumer electronics education is essentially funded by advertising placed by the providers of phones, devices, appliances, and so forth. In general, online platforms do not advertise as such, so there is a policy opportunity to see how such resources can be developed in the marketplace. Consumer education on privacy could help consumers understand the principles of consent and control and exercise their associated freedoms.

¹⁵ Willis, Lauren E. "Evidence and ideology in assessing the effectiveness of financial literacy education." *San Diego L. Rev.* 46 (2009): 415

¹⁶ Connell, David B., Ralph R. Turner, and Elaine F. Mason. "Summary of findings of the school health education evaluation: Health promotion effectiveness, implementation, and costs." *Journal of school health* 55.8 (1985): 316-321.

¹⁷ Supra Willis

Public Choice Explanation for the Lack of Consumer Education on Privacy. The academic discipline of public choice uses economics to investigate problems in political science. It could help explain why consumer education on privacy is lacking, aside from one possible explanation that consumers are not interested to learn about privacy and therefore do not demand such information. A public choice theorization would likely recognize that while the notion of consumer education has implicit valence, industry and regulators may have incentives to de-emphasize education. Indeed, if consumers are empowered to make informed choices, they have less need of regulatory supervision. Similarly, consumers making informed choices also affects industry; it has a powerful effect to drive consumers from one firm to another.

The GDPR is suspect in that among its 173 provisions the role and importance of consumer education is never discussed.¹⁸ This is a serious oversight particularly when the EU's official cybersecurity research institute noted the primacy of consumer education to create privacy, accountability, and trust.¹⁹ Nor is consumer education discussed in the context of the California Consumer Privacy Act. This is likely because the real objective for these regulations is not empower consumers but to strengthen the data protection and compliance business, specifically to give jobs to data protection officers, regulators, and litigators.

The assumption of the European and Californian rules is that regulatory authorities have more information than consumers and firms and therefore know better how to order transactions in the marketplace.²⁰ All the same, these regulations impose massive new responsibilities on data protection agencies without a concurrent increase in training or funding.²¹ Data regulators must wear many hats, including "ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer."²² Furthermore, these regulations widen the gap between the high expectations for data protection and the low level of skills possessed by data supervisors charged with its implementation.²³ There are certainly many talented individuals among these

¹⁸ Layton, Roslyn, How the GDPR Compares to Best Practices for Privacy, Accountability and Trust (March 31, 2017). Available at SSRN: <https://ssrn.com/abstract=2944358> or <http://dx.doi.org/10.2139/ssrn.2944358>.

¹⁹ Claude Castelluccia and more, "Privacy, Accountability and Trust – Challenges and Opportunities — ENISA," Report/Study, Enisa, February 18, 2011, <https://www.enisa.europa.eu/publications/pat-study/>.

²⁰ See generally F. A. Hayek, "Economics and Knowledge," 1937; and F.A. Hayek, "The Use of Knowledge in Society," 1945.

²¹ Douglas Busvine, Julia Fioretti, and Mathieu Rosemain, "European Regulators: We're Not Ready for New Privacy Law," Reuters, May 8, 2018, <https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1915X>.

²² Colin J. Bennett and Charles Raab, "The Governance of Privacy: Policy Instruments in Global Perspective," 2006.

²³ Charles D. Raab and Ivan Szekeley, "Data Protection Authorities and Information Technology," *Computer Law and Security Review* (forthcoming), <https://ssrn.com/abstract=2994898>.

ranks, but the mastery of information communication technologies varies considerably among these professionals.

Public choice theory also suggests that the data regulators' preferences are not necessarily aligned with the "public interest," or what is best for consumer welfare in the long run. Increasing user knowledge and the quality of data protection technology could legitimately make people better off, but it could also render regulators less important. While data regulators will not necessarily reject policies that improve user knowledge and technology design, it is in their interest to promote inputs that increase their own resources and legitimacy in conducting compliance and adjudication.²⁴

Surveys demonstrate that many users fail to practice basic privacy-enhancing behaviors.²⁵ This situation is ripe for improvement and represents a classic example of how consumer education can improve outcomes better, more quickly, and at a lower cost than regulation. Indeed, the first principle of consumer education in data protection, buyer beware, is the same first principle for how citizens should protect themselves in cyberthreats in Michael Chertoff's new book on cybersecurity: "Be mindful of what data you transmit and what you connect to your own network."²⁶ He also recommends practicing cyber hygiene, taking advantage of layered cybersecurity technology, and outsmarting scams with a phone call.

Consumers need to practice the same kind of vigilance and personal responsibility in cybersecurity as they do in the data protection domain. Outsourcing the job to bureaucrats will not cut it, as the user can be a vulnerability point. Consider warnings and labels on food and chemicals; while regulation can mandate that disclosures be made, if users do not recognize the meaning of expiration dates or consumption warnings, then disclosure has little impact.

Transparency. The principle that "organizations should be **transparent** about how they collect, use, share, and store users' personal information" is laudable. Indeed, the FTC has been extremely deft to use transparency rules to bring actions against actors which threaten and/or harm consumers. The agency has levied significant fines and collects compensation for users. The history of enforcement serves as an important deterrent as well as a roadmap for firms.²⁷

²⁴ Roslyn Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust," March 31, 2018, 14, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944358.

²⁵ Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust."

²⁶ Michael Chertoff, "Exploding Data: Reclaiming Our Cyber Security in the Digital Age," *Atlantic Monthly Press*, 2018.

²⁷ "Privacy and Security Enforcement," Federal Trade Commission, July 22, 2013, <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement>.

The bottom line for policymakers is that the FTC has proven its capability to police privacy and security, and transparency requirements are powerful tools to protect privacy.

However imposing transparency requirements is not without costs to consumers. The GDPR is driving disclosure overkill. Indeed, European requirements have become so onerous that many consumers have stopped using websites with cookie disclosures.²⁸ Opera, the popular browser, has developed technology to block the disclosure dialogues that plague users every time they visit a website in EU. Indeed, technologies and users can find innovative ways to go around regulations they don't like.²⁹

Policymakers should not believe that automatically making consent more explicit makes consumers more informed. If the user fundamentally does not understand to what she agrees or the underlying transaction, no amount of disclosure, however detailed or granular, empowers the user. This is the gap that consumer education can fill.

When producers and consumers do not have perfect information, this discrepancy can give rise to inefficiency or abuse. Peer-to-peer platforms have resolved many of these problems of informational asymmetry through information sharing. Consider how the ability to evaluate drivers and riders is an essential part of ridesharing apps. Before Uber, neither the taxi company nor the regulator was interested to publish real-time information about the quality of drivers or cars, as it could impugn the deficiency of regulator. Ratings and peer reviews are essential in the digital economy. Indeed, some health regulators use Yelp ratings to help inform how they deploy their inspection resources.³⁰

Consumer education could be vital to demystify the “black box” of many internet platforms, which for many consumers is a system in which they can observe the inputs and outputs but have little to no insight to its internal workings. It is only when consumers have enough education about the tools they can use that they can begin to “exercise **control** over the personal information they provide to organizations.”

²⁸ Daniel Castro and Alan McQuinn, The Economic Cost of the European Union's Cookie Notification Policy, ITIF, Nov. 6, 2014, <https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy>.

²⁹ Adam Thierer and Chand Reese. “Evasive Entrepreneurs and Permissionless Innovation. The Bridge. Sep 11, 2018 <https://www.mercatus.org/bridge/commentary/evasive-entrepreneurs-and-permissionless-innovation>

³⁰ Roslyn Layton, “How Sharing Economy Regulatory Models Could Resolve the Need for Title II Net Neutrality,” AEI, June 26, 2017, <http://www.aei.org/publication/sharing-economy-regulatory-models-resolve-need-title-ii-net-neutrality/>; And Arun Sundararajan, *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism* (MIT Press, 2016)

Preliminary ideas about promoting consumer education in privacy. My submission to the FTC describes some of the leading privacy education programs beginning on page 15.³¹ Firms could support these organizations financially to spread the information and as an example of their commitment to principles. Following are additional ideas to consider to embedding consumer education for privacy into the marketplace.

- Leverage the FTC’s educational website, materials and knowledge into the public domain <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. Firms could link to the FTC from their websites.
- Firms can develop their own educational platforms for privacy and engage and encourage customers to learn.
- Firms could offer rewards/discounts for customers to take online privacy training.
- Firms could supplement disclosures with consumer-centric tools (videos, cartoons etc.) to explain how their products and services, incorporate data.
- A task force of FTC, industry and consumers could promote consumer education for privacy.

Transparency and consumer education are important so that consumers can make informed decisions about whether they want to use one service versus another. Indeed, consumers may well say that they don’t want to use a certain service because they are not comfortable with the provider’s practices. The suggestion of supporting consumer education for online privacy follows the experience with initiatives in health education and financial literacy. If we want people to value privacy, they should be able to access tools and resources which explain why it is important and how, in basic terms, online business models work.

If companies violate their contracts and terms of service, using data that is not disclosed and/or without consent, these violations can and should be processed by the Federal Trade Commission. Improving the FTC’s enforcement capabilities overall, notably with removing common carrier and non-profit exemptions, increasing the FTC’s budget and headcount for online privacy investigations and enforcement, and allowing the FTC to levy civil penalties, would be helpful on this issue.

The Honorable Michael C. Burgess, M.D.

³¹ https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf

1. One of my concerns with the online ecosystem is transparency -- how companies tell their consumers about their collection and use of personal data. Terms of services are too long and too complicated for anyone to reasonably read.
 - a. Dr. Layton, in your testimony you state that there is no consumer protection without consumer education. What should we be thinking about in Congress to improve consumer education initiatives?

Answer:

Please see answer to question posed by Representative Eshoo on p. 6.

2. Dr. Layton, I recently heard from a small business in Dallas/Ft. Worth, called Ultimate Ventures, that specializes in business meetings, events and logistics. This small business does not normally deal with a lot of consumer data, and is now being asked to sign a "data protection agreement" from a client based on the GDPR that -- in the words of the President of the business -- is "not simply daunting, but is impossible to agree to" and that there is "no way" for the company to agree to everything in the agreement.
 - a. What would it mean for small businesses in the U.S. if we follow suit and adopt a framework similar to GDPR?

Answer:

My Senate testimony³² detailed the 10 harms of the GDPR (and CCPA) already documented which include

1. Rules promised to level the playing field have strengthened the largest players.
2. Small and medium sized firms have weakened as a result of the GDPR, the opposite of the promised effect.
3. The GDPR has silenced free speech and expression.
4. The GDPR has proven cost prohibitive for many firms.
5. The GDPR threatens innovation and research.
6. The GDPR has created cybersecurity threats.

³² <https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf>

7. The GDPR and the CCPA create risks for identity theft and may incentivize fraud.
8. The GDPR, however well-intentioned, has tricked people into thinking that they and their data are now more private and safe, when they are not.
9. The GDPR and the CCPA use the pretense of customer sovereignty to increase the power of government.
10. The GDPR and the CCPA fail to incorporate the role of innovation and education, factors which ultimately create better privacy systems and empower users to make informed decisions.

All these outcomes have either a direct or indirect impact on small business. In summary, we have seen that as a result of the GDPR, the large advertising platforms have gained market share; smaller advertising competitors have lost market share; small firms have stopped serving markets because of the cost and uncertainty of regulation; and small firms have been disincentivized to pursue technical means which could ultimately improve privacy because of the lack of a safe harbor to test new technologies.

- b. What concerns do you have with the California privacy law and its effects on small businesses?

Answer:

The costs of the CCPA is likely to be at least four times its benefits. Firms are spending a minimum of \$100,000 today to comply with the CCPA. It is expected that there are half a million firms liable under the CCPA; they are overwhelmingly small to medium sized businesses; most spend but a few thousand dollars annually on their information technology operations and likely have zero budget for privacy regulation. Even with the minimum revenue threshold, the CCPA will cause many firms to do one of the following: 1. Stop serving California; 2. Look for a buyer or another form of exit; 3. Close down. The CCPA is particularly unfair because it was conceived to discipline giant Silicon Valley firms with market caps that exceed the gross domestic product of most countries, but its many requirements fall the hardest on small and medium sized firms which, not only do not have budget to pay for costly software upgrades and privacy

lawyers, but have not compromised the privacy of their users. It is not the first time that regulation promised to protect consumers ends up rewarding large, incumbent industries.³³ This dynamic has been experienced with the airline, telephone, and train industries, and California policymakers now make the same mistake with internet platforms.

The preliminary analysis for the benefit cost of the CCPA is available at <http://www.aei.org/publication/the-costs-of-californias-online-privacy-rules-far-exceed-the-benefits/> and follows below.

Cost-benefit analysis (CBA), while imperfect, improves policymaking. However, CBA is frequently performed after the fact to justify regulatory decisions already made. Some reject CBA outright, saying that costs and benefits are too difficult to quantify, or because its conclusions do not support predetermined policy preferences. To overcome quantitative and cognitive difficulties, economists propose “back of the envelope” CBAs, ensuring that analysis is done *before* rulemaking and incorporates observed values policymakers can understand. George Washington University’s Daniel Pérez recently presented a preliminary CBA in light of privacy regulation from Europe and California.

Benefits of privacy regulation

Pérez attempted to find the best case for regulation. He assumed one in four mobile users would take advantage of privacy regulation based on reported willingness to pay (WTP) for the privacy of personally identifiable information using techniques for concealing browser history and geolocation data and for the ability to access, correct, and transfer personal data. His model for mobile apps accessed by Android users in the US builds on frameworks developed by Hann et al. (2007), Savage and Waldman (2013), Acquisti et al. (2013), and Fuller (2019). The benefits are calculated by WTP for a typical privacy configured app (\$3.47), the average number of apps per user (23), the lump sum WTP for privacy functionality (\$13.77), and the number of smartphone users willing to pay for such services (generously estimated to be 25 percent of 257,300,000 smartphone users). Importantly, apps are downloaded in year one with updates in future years. This calculation yields an upfront benefit of \$8.6 billion and \$6.1 billion in the following years. With discounting, the accumulated benefit is between \$48 and 56 billion in a decade.

³³ Should tech giants be more heavily regulated? Debate in Economist.com 30 April – 7 May 2018. Follow up mention on “Open Future” <https://www.economist.com/blogs/openfuture/2018/05/open-future>

These benefits seem small, especially relative to the \$1.6 trillion digital economy, but the numbers are not out of line with other studies of discrete privacy rights from Europe's General Data Protection Regulation (GDPR). Indeed, studies of users' willingness to pay for an ad-free Facebook suggest similar amounts. Forty-two percent of respondents said they would pay up to \$5 per month, a quarter would pay up to \$10, and one-third would pay \$11 or more). These numbers correspond to Facebook's average revenue per user per month of \$11 in Q4 2018, the value that Facebook earns on advertising and other services divided by the number of users. This figure presumably includes the "risk" people undertake to use Facebook. Despite many policymakers' doomsday scenarios following the Cambridge Analytica scandal and the 2016 election, Facebook's revenue and usage has increased in all geographies in the past two and a half years.

Costs of privacy regulation

While Pérez generously estimates the benefits of privacy regulation, he conservatively estimates the costs at \$24.5 billion for upfront compliance and lost advertising revenue. The present value of the annualized costs are \$57 – \$63 billion in the coming decade. When balanced against the benefits, the outcome is a total loss of \$7 – \$8 billion.

If the actual costs from the GDPR are any indication, the real costs of the California Consumer Privacy Act (CCPA) are likely to be much higher. Six months after the implementation of the GDPR, 41 percent of firms surveyed by Verasec reported that compliance cost had exceeded their budgets.

We also can examine the compliance costs already being borne by California firms preparing for the CCPA. TrustArc commissioned a survey of the readiness of 250 firms serving California from a range of industries and company size in February 2019. It reports that 71 percent of the respondents expect to spend at least six figures in CCPA-related privacy compliance expenses in 2019 — and 19 percent expect to spend over \$1 million. Notably, if CCPA were in effect today, 86 percent of firms would not be ready. An estimated half a million firms are liable under the CCPA, most of which are small- to medium-sized businesses. If all eligible firms paid only \$100,000, the upfront cost would already be \$50 billion. This is in addition to lost advertising revenue, which could total as much as \$60 billion annually.

Conclusions

Conservatively, costs of privacy regulation exceed benefits by four fold. Some claim that benefits could increase because of fines and lawsuits. While this could be true, the substantive fines

would come from only a few firms that could be prosecuted under existing laws and consent decrees. In any case, payouts wouldn't be realized for years due to the litigation sure to ensue. In the meantime, all firms would have to bear increased costs, and many would exit, leaving larger firms greater market shares, as already experienced with the GDPR.

Because people don't pay out of pocket for most apps today and already have the option to turn off tracking, it remains to be seen if even modest benefits of \$6 – \$9 billion annually are realized. Under the California framework, users inevitably will have fewer apps to choose from as the long tail of advertising-supported apps will be cut. Pérez suggests a radical idea that privacy legislation should be based on evidence that regulation will actually advance privacy outcomes in ways that consumers value. The lion's share of the money generated by the regulation flows to software upgrades, privacy consultants, and lawyers — not consumers.

Small Business Testimony to the Senate

Sen. Jerry Moran, (R-KS), Chairman of the Subcommittee on Manufacturing, Trade, and Consumer Protection, convened a hearing on Small Business Perspectives on a Federal Data Privacy Framework. The testimonies of this hearing are worthy of review. Here are a few of the highlights. Here are some of the perspectives shared at the hearing.³⁴

National Association of Realtors

Nina Dosanjh, Vice Chair of the Technology Policy Committee of the San Francisco based National Association of Realtors (San Francisco) observed, "Realtors, like many main street businesses, rely on data to enhance revenue and drive efficiency, whether by better understanding the needs of existing customers, reaching new ones, or obtaining valuable insights to guide a wide array of business decisions. For example, realtors may use consumer data to allow them to advise their selling clients on how to price their home and how many potential buyers will be interested at different price points. It can also be used to give buyers a better sense of what types of properties competing home buyers are looking at, as well as their buying ability. In sum, realtors use the consumer data they collect to improve their clients experience in a way that consumers can understand and expect."

Silver Star Communications

³⁴ <https://www.forbes.com/sites/roslynlayton/2019/03/26/congress-investigates-whether-privacy-rules-can-protect-consumers-without-killing-small-business/#7217e9c34459>

Jefferson England the CFO of Silver Star Communications, headquartered in Thayne, WY, explained the need for a single federal standard that allows for companies to serve their customers. "We provide services in multiple states, and having to manage a patchwork of state privacy laws will not only create an environment of uneven protections, but would create administrative burdens on small business," he said. "Legislation should not interfere with business and consumer relationships that are based on mutually understood privacy protection tolerances. If a consumer is willing to release data in order to receive services, it should be the consumer's right to do so, and the business should be allowed to provide such services. Similarly, the market should be allowed to present data privacy alternatives as competitive differentiation so long as data privacy protection practices are clearly identified and accepted by the consumer."

Engine Advocacy and Research Foundation

Evan Engstrom, Executive Director, Engine Advocacy and Research Foundation, the so-called voice of Silicon Valley startups, suggests maintaining the spirit and good intentions of the CCPA without its heavy-handed prescriptions. His testimony offers highly detailed assessment of the regulatory impact to startups and details the impact to date of the GDPR. He observes, "... as state and federal policymakers look to bolster privacy protections for consumers, there is a very real risk that the end result will be a complex regulatory landscape that startups on bootstrap budgets can't afford to comply with, especially compared to large companies with massive budgets and legal teams. Rules that are ostensibly pro-privacy could end up cementing the market power of those very Internet giants whose behavior sparked much of these conversations. . . We've seen this with the European Union's General Data Protection Regulation, where many small companies left European markets or abandoned plans to expand to European markets rather than face the costly compliance burdens. In fact, there's concrete evidence that GDPR gave the big Internet companies a boost in Europe. According to one survey, Google's ad tracker actually saw an increase, albeit small, in reach since GDPR went into effect ten months ago. Facebook's ad tracker saw a small decrease, but everyone else saw significant losses. GDPR's extensive and complex obligations created new compliance burdens that large incumbents could bear but resource-constrained startups could not. Policymakers should enshrine consumer privacy protections in law, but they must work to ensure far-reaching rules promote consumer welfare without harming competition."

Engstrom details the many ways that the CCPA threatens startups including but not limited to

1. The overly broad definition of personal information that does not explicitly exclude de-identified and aggregated data

2. The CCPA defines “sale” expansively, covering many commonplace practices that businesses rely on to provide goods and services to consumers.
3. The prohibition on differing service based on consumer privacy choices. In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups.
4. Privacy and security problems with CCPA’s right to access and delete which create opportunities for fraud or needless requirements for additional data collection.
5. The private right of action creates uncertainty for startups. No matter how thorough a company’s data security practice safe, determining whether they were legally “reasonable” is not amenable to early adjudication in a lawsuit.
6. CCPA’s small business exemption fails to capture startups.
7. The design and procedure of the opt-out function does not sync with startups practices
8. The CCPA imposes significant compliance burdens for the diverse business models represented in California’s startup ecosystem.

Kansas City Tech Council

Ryan Weber, President of the Kansas City Tech Council dispelled the view that big data is only something for Silicon Valley firms, "Algorithms are the backbone of most modern technology applications, and algorithmic thinking is necessary when considering the future of federal data privacy laws. Conditional algorithms use IF-THEN decisions between two courses of actions. For example, IF a company, no matter the size collects sensitive data, THEN it must comply with federal data privacy laws and meet certain cybersecurity standards set forth by the appropriate regulatory agency. As technology continues to advance and find its way into every industry, business sector, and company, we must remember, not all technology is created equal and not all data should be treated the same. Accountability will make federal data privacy laws effective. The agency responsible for upholding these laws should be allowed to adjust fines and penalties equal to the violation. This sentiment is shared by our member companies. Other global examples of privacy laws, such as General Data Protection Rights (GDPR), set fines at such a high-level many small and startup companies cannot afford."

The Honorable Richard Hudson

1. Dr. Layton, the California law does not allow a company to deny, or charge a different price, or offer a different quality of goods or services to consumers who do not want a company to collect data. This raises some government takings questions but how will this impact lower income families? Will companies be forced to provide free services to California consumers, paid for by the rest of America?

Answer:

Thank you for asking this important question, which does in fact implicate government takings. It also reflects many privacy advocates' absolutist view of privacy rights which threaten to eclipse other rights, notably an individual's right to decide for himself or herself what kind of business model she wants to access.³⁵ The prohibition on commercial freedom in the CCPA is a feature designed by CCPA advocate Alastair MacTaggart who described in his questioning in his Senate hearing that he took offense that his local Supercuts salon requesting his email and phone upon checking in for an appointment.³⁶ MacTaggart called it "out of control" and intimated that this practice should be eliminated for all Supercuts customers. (He also spent nearly \$3.5 million of his own fortune from a successful real estate business, which, ironically, relies on the same kind of data processing he now wants to eliminate.) This kind of elitism fails to see how many people appreciate SMS reminders for their salon appointments and want to receive email offers of coupons for hair care products, discounts, and so on.

When the law requires a firm to provide a service without collection of data it creates a free rider problem in which those who consent to data collection must endure increased data collection and processing to compensate for those who don't consent. As such, it unfairly burdens consenting users to higher burdens and costs without commensurate benefit. More generally, it decreases the parameters of competition, precisely the innovative ways which small firms could differentiate with data in order to gain a foothold in the marketplace.

The question alludes to fundamental theories of privacy. Online privacy can be seen from two competing paradigms. One model is that of rational choice, in which the individual weighs the cost and benefits of privacy and decides whether to transact. The other view paints users as being at the mercy of external factors that determine whether they reveal or conceal themselves. The former tends to support solutions and technologies that empower consumers to make their own choices and suggests that firms, valuing their customers, will take proactive steps to steward their experience. The latter holds that privacy tools are inevitably unreliable and that firms take predatory advantage of users. According to this view, regulation is needed to keep firms in check and to protect consumers.

³⁵ <https://www.libertarianism.org/building-tomorrow/protecting-data-privacy-without-destroying-the-internet>

³⁶ <https://www.commerce.senate.gov/public/index.cfm/hearings?ID=3A98134B-6CCE-4491-B22B-BC831C3DFF5D>

Empirical tests of the two models show that consumers are not inevitably predisposed to making bad choice or failing to act in a privacy enhancing matter.³⁷ Research from tools deployed among hundreds of millions of users shows that privacy preferences change minute to minute depending on the site visited, the user's goal, and the user's desire for security and speed.³⁸ As such, the opt-in regime is not empirically demonstrated as superior means of protecting the user's privacy. The point is merely that privacy is not a binary choice. There are many means and modes to secure, and its importance varies depending on the user and the situation. As such, policymakers should tread carefully before applying draconian regulations that may satisfy the most vocal privacy advocates but reduce benefits and utility for millions of consumers.

Notably a review of the literature on the impacts of economic regulation in the information communications technology sector shows a detrimental impact of regulation on innovation.³⁹ Regulation can create a deadweight loss in the economy as resources are diverted to regulatory compliance and away from welfare-enhancing innovation. A study across all major industries from 1997 to 2010 found that less-regulated industries outperformed overregulated ones in output and productivity and grew 63 percent more. Overregulation increases barriers to entry for entrepreneurs, which slows economic growth.⁴⁰ Moreover, regulation can crowd out efforts to create new and better systems.⁴¹ For example, under the GDPR firms must employ privacy professionals, reducing revenue for engineers who can design and deploy privacy professionals.

Notably Engine Advocacy and Research Foundation has answered this question in its testimony to the Senate Commerce Committee, calling it "Prohibition on differing service based on consumer privacy choices."⁴² They declare,

CCPA prohibits companies from offering different prices or levels of quality of products and services to consumers who exercise their rights under the law, including

³⁷ Idris Adjerid, Eyal Peer, and Alessandro Acquisti, "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," April 14, 2016, <https://ssrn.com/abstract=2765097>.

³⁸ Scott Meyer, "The Next \$50 Billion Will Come From . . . Putting Users First," Ghostery Inc., <https://www.slideshare.net/ghosterybrand/the-next-50-billion-will-come-fromputting-users-first>.

³⁹ Luke Stewart, "The Impact of Regulation on Innovation in the United States: A Cross," Information Technology and Innovation Foundation, June 2010, 18, <http://www.itif.org/files/2011-impact-regulation-innovation.pdf>.

⁴⁰ Antony Davies, "Regulation and Productivity," Mercatus Center, May 7, 2014, <https://www.mercatus.org/publication/regulation-and-productivity>.

⁴¹ Patrick McLaughlin and Richard Williams, "The Consequences of Regulatory Accumulation and a Proposed Solution | Mercatus," Mercatus Center, February 11, 2014, <http://mercatus.org/publication/consequences-regulatory-accumulation-and-proposed-solution>.

⁴² https://www.commerce.senate.gov/public/_cache/files/949f1fc8-dc28-4760-9f47-6cb925a1549e/0AE3566F5899E50A6C4D08C7142D8752.testimony-of-evan-engstrom-engine.pdf

the right to opt-out of data sharing. In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups. Unlike large Internet companies that have been offering ad-supported free services for years, a startup entering the market will have a harder time getting new users who are unfamiliar with the company to pay for its products and services. Even if a startup can get some users to pay, the law would effectively require every ad-supported company to take on the burdens associated with establishing a payment processing system in case some users decide to opt-out. At the same time, a small company will have significantly fewer opportunities to offset the costs of offering a product or service for free using revenue streams from other parts of its business, while bigger companies are better positioned to take a loss on offering a free product or service. The law does allow companies to charge a different rate or offer a different level of products or services so long as “that difference is reasonably related to the value provided to the consumer by the consumer’s data.” While this phrasing is likely a drafting error and obviously unworkable—how could a company know how much an individual consumer values his own data?—even a generous reading of the law’s presumed goal would present existential problems for small startups. Even if companies are forced to provide service to consumers who opt-out of data sharing practices that are fundamental to the company’s business model, but are allowed to recoup the lost value directly from consumers by charging a different price or offering a different level of service so long as that difference is reasonably related to the value provided to the company by the consumer’s data, startups would have a very difficult time estimating or defending in court what would constitute a price or quality difference that’s “reasonably” related to the value of a consumer’s data. As startups launch and grow their businesses, there’s typically not an immediate, obvious value that can be clearly assigned to individual pieces of data supplied by consumers. Even if a data set has an explicit value in the eyes of investors, data associated with any particular consumer typically does not hold much value on its own.

Even worse, this non-discrimination provision would require every company that shares User data to build the infrastructure to process customer payments in the off chance that a particular consumer opts-out of the company’s data practices but wishes to pay a “reasonably related” fee instead. Larger companies might be able to bear the increased overhead of payment processing, but smaller startups will not.

Attachment—Additional Questions for the Record

Ms. Denise Zheng, Vice President, Technology, Innovation, Business Roundtable

The Honorable Michael C. Burgess, M.D.

1. One of my concerns with the online ecosystem is transparency -- how companies tell their consumers about their collection and use of personal data. Terms of services are too long and too complicated for anyone to reasonably read.
 - a. Ms. Zheng, do you agree that companies can do better to help consumers understand their terms of service and how they are using data? Do you have any examples of companies who are thinking outside of the box on this issue?

Yes, I agree that more can be done to help consumers understand the terms of service and how data is used. Consumers should have access to clear, understandable statements about the organization's practices and policies with respect to personal data. These statements should include information on the types of personal data collected; the purposes for which the personal data will be used; whether and for what purposes personal data may be disclosed or transferred to non-affiliated third parties; the choices and means for exercising individual rights with respect to personal data; and the contact details of persons in the organization who can respond to questions regarding personal data. Many Business Roundtable member companies are applying innovative approaches to provide consumers with information and tools they need to more easily understand how their data is collected and to exercise more control over their personal data. I would be happy to follow-up with your staff to discuss more specific examples.

The Honorable Richard Hudson

1. Ms. Zheng, among the objectives of a privacy law highlighted by the Business Roundtable are fostering innovation and protecting competition. How should we consider striking the right balance between ensuring consumers information is protected, but not creating an environment where we impede innovation and growth?

Innovation thrives in a stable policy environment where new ideas can be explored and flourish within a well-understood legal and regulatory framework. A state-by-state approach to regulating consumer data privacy threatens to undermine innovation in the United States. It is important for federal privacy legislation to establish a consistent set of protections for consumers that replaces the patchwork of state privacy laws. To enable continued innovation, any rulemaking authority that may be considered in privacy legislation should be narrowly scoped and require the regulatory agency to analyze the costs, benefits, and impact on innovation before any new rules are enacted.

Questions for the Record

House of Representatives Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce

Hearing on *Protecting Consumer Privacy in the Era of Big Data*

David F. Grimaldi, Jr., Executive Vice President, Public Policy, Interactive Advertising Bureau

The Honorable Robin L. Kelly:

In the wake of the repeal of broadband privacy rules last year, what are your thoughts on privacy proposals including ISPs. For example, should ISPs be able to mine DNS data? Are there any other solutions to this that could protect consumers from these privacy violations if we don't come up with a regulatory one?

Consumers want strong privacy protections that apply consistently to their data across the Internet, regardless of what state they happen to be in or what entity is holding the data, as evidenced by a Peter Hart survey confirming that 94% of consumers want the same protections to apply to their online information regardless of the company that collects or uses it.¹

ISPs should of course be included in any federal privacy legislation, but a cornerstone of federal legislation should be that there are consistent obligations imposed on all entities that collect and use consumer data.

ISPs have made a number of enforceable public commitments not to sell or monetize sensitive user data without express customer consent, and to be transparent with their customers regarding how their information will be used, shared, protected.²³

At the same time, ISPs need to access and use information like DNS information to deliver their services, to keep their networks and users secure, and to improve their services and develop new ones. A law that follows the basic principles I set forth in my testimony before the Committee – focusing on the risk of harm to the consumer and not on the identity or business model of the marketplace participant – is the best way to ensure that any problematic practices are prohibited, while allowing pro-consumer, pro-privacy practices to flourish.

Companies understand the importance of privacy to consumers, and they are working on a number of different fronts – including through open standards organizations – to identify ways to improve privacy and security standards, which they can then integrate into their products and services regardless of the

¹ <https://www.progressivepolicy.org/issues/economy/ppi-poll-recent-national-survey-internet-users/>

² <https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf>

³ <https://www.ncta.com/positions/isp-privacy-principles>

regulatory regime. With respect to DNS, for example, the Internet Engineering Task Force (IETF) – the premiere organization for developing the standards that serve as a technical foundation of the Internet – recently developed two new DNS protocols -- DNS over TLS and DNS over HTTPS -- that will enable the encryption of DNS queries. ISPs are currently examining these new protocols to determine whether, and, if so, when and how to deploy them.

The Honorable Richard Hudson:

Mr. Grimaldi, in your testimony you highlight that small businesses and startups have seen the negative impacts of GDPR. Have companies exited Europe because of GDPR? If so, can you please explain why that is and what we can do to ensure we maintain a regulatory environment in the U.S. that allows businesses to grow?

Following the implementation of the GDPR, many U.S.-based companies and publishers chose to exit the European market instead of risk the significant fines related to potential GDPR violations.

Jeff South of the Nieman Foundation for Journalism at Harvard University reported that nearly one out of three of the 100 largest U.S. newspapers were no longer available in Europe more than two years after the law was passed.

The decision to exit the European market has not been confined to large U.S. publishers. As of March 20, 2019, 1,129 U.S. websites, including many small newspapers and online services, are still unavailable in the European Union following the implementation of GDPR.⁴ This includes companies such as The Fayetteville Observer, North Carolina's oldest newspaper which traces its roots back to 1816.⁵

Additional evidence suggests that the negative impact of GDPR has been most acutely felt by smaller U.S. businesses. In the digital advertising industry, one study has indicated that smaller advertising companies have lost between 18 percent to 31 percent in market share since GDPR went into effect, while market leaders have gained in reach over that same period.⁷

While well intentioned, we believe GDPR imposes significant burdens on businesses while failing to stop many practices that are truly harmful. Furthermore, GDPR fails 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.

IAB recommends that as an alternative to GDPR, a new U.S. federal privacy law should impose clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified in the law. Furthermore, such a law 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.

⁴ <https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr>

⁵ <https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr>

⁶ https://www.fayobserver.com/about_us

⁷ <https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr>

In this way, we believe the U.S. can provide meaningful protections to all Americans while ensuring U.S. businesses of all sizes and across all industries are able to compete and grow.

Questions for the Record
 Nuala O'Connor, President and CEO
 Center for Democracy and Technology

Protecting Consumer Privacy in the Era of Big Data
 Subcommittee on Consumer Protection and Commerce
 House Energy and Commerce
 February 26, 2019

1. In the wake of the repeal of broadband privacy rules last year, what are your thoughts on privacy proposals including ISPs. For example, should ISPs be able to mine DNS data? Are there any other solutions to this that could protect consumers from these privacy violations if we don't come up with a regulatory one?

The United States should have a universal privacy law that applies to all actors, including internet service providers (ISPs) and other types of businesses, online and offline. People should be able to rely on basic protections that follow their data no matter who holds or processes it. The repeal of the broadband privacy rules in 2017 adds to the urgency of passing comprehensive privacy legislation. ISPs have access to and process highly sensitive personal information by virtue of providing a vital location-based service. Privacy legislation should protect much of this information from secondary uses, which in the context of ISPs means uses that are not required to provide the internet access or other services which a consumer has chosen. CDT's draft legislation contains several key data use and sharing prohibitions that would protect broadband customers, but that, more importantly, would also apply to the entire data ecosystem.

First, our proposal prohibits the processing of precise geolocation information if it is not required to provide the service a person has requested (such as broadband internet service). Data that customers send to ISPs by virtue of using the internet can reveal their location. To the extent that this location information is precise (within 1,750 feet), our bill would prohibit any entity from collecting, sharing, selling, or otherwise processing it except as necessary to provide the service.

Second, our proposed bill allows the processing of health information only when it is necessary to provide the service a person has requested, such as a health or fitness tracking app or a symptom-checking tool. This means companies may process information as necessary to provide and optimize broadband service, but may not harvest health data and share it with advertisers. A person's browsing and app usage history—the websites and pages they visit, search history, and names or categories of apps they use and information they send to those apps—can reveal personal health information (for example, if a person is reading about a particular health condition, purchasing healthcare products, using a wearable fitness device or sleep tracking app). Consumers should be able to access health-related information and services without worrying that this information could end up in the hands of third parties, be

used to serve them third-party ads, or determine the types and rates of insurance or credit for which they qualify.

Third, our proposed legislation prohibits the sale or licensing of the contents of or parties to communications. This would include browsing information, such as the websites a person visits, the messages (such as emails, texts, and instant messages) they send, and the individuals they communicate with. The sale of browsing history was a central concern that led the Federal Communications Commission (FCC) to write broadband privacy rules. Many different types of companies and services process browsing history, and it should be protected regardless of the type of entity processing it.

Domain Name System (DNS) data can reveal the contents of people's online activities, including the websites they visit. This type of data would be covered by the secondary use prohibitions in CDT's draft legislation.

While individuals may be able to take certain steps to obscure some of their browsing history, such as using a virtual private network (VPN), no self-help solution can give people complete control over the sensitive personal information that they must reveal in order to participate in digital life. VPNs themselves are provided by companies that customers must trust to protect their information. Even when websites encrypt their traffic, DNS data can still reveal nuanced information about people's activities. Ultimately, Congress must pass legislation to limit the behavior of ISPs and all other entities that process personal information.

2. Many proposals direct the FTC to establish rules to address advertising practices that result in discrimination. Do you have ideas in mind for what kind of rules the FTC could put in place?

The Federal Trade Commission (FTC) should request and analyze corporate information about advertising targeting practices and develop rules that address discriminatory or otherwise unfair advertising practices. Because there is a lack of transparency into the online advertising ecosystem, more information is needed to fully understand the types of data collection, aggregation, sharing, profiling, and targeting practices that result in discrimination or exploitation. The FTC has indicated that it intends to launch a study of platforms' data practices. The activities of advertising networks, data brokers, and advertisers themselves must also be considered.

Some findings about discriminatory advertising and potential responses are beginning to emerge through litigation. Last week, Facebook reached a settlement in lawsuits alleging that its practices relating to the advertising of jobs and housing violated civil rights laws. As part of the settlement, Facebook agreed to several changes, including creating a separate portal for users placing job, credit, and housing ads, which will restrict targeting options. Advertisers in these categories will no longer have the option of excluding people based on age, gender, zip code, and several other categories. Facebook will also create a portal where users can search and view all current housing ads that have been placed, regardless of the advertisers' targeting

choices. Facebook will also allow the National Fair Housing Alliance to engage in testing of the platform to ensure that these reforms are effective. While these are first steps that only address one part of the market for potentially discriminatory advertising, they are measures whose effectiveness the FTC can observe over the next several months or years as the agency crafts rules. In particular, the ability to test or audit companies' practices has long been a critical aspect of enforcing civil rights laws in the brick and mortar world, and we would encourage the FTC to consider how testing can and should be done online.