S. HRG. 116–619

EXAMINING LEGISLATIVE PROPOSALS TO PROTECT CONSUMER DATA PRIVACY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

DECEMBER 4, 2019

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
52–801 PDF WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ROGER WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington, *Ranking*
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

JOHN KEAST, *Staff Director*
CRYSTAL TULLY, *Deputy Staff Director*
STEVEN WALL, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

CONTENTS

	Page
Hearing held on December 4, 2019	1
Statement of Senator Wicker	1
Statement of Senator Cantwell	3
Letter dated December 3, 2019 to Hon. Roger Wicker and Hon. Maria Cantwell from Richard Hunt, President and CEO, Consumer Bankers Association	5
Letter dated December 3, 2019 to Hon. Roger Wicker and Hon. Maria Cantwell from Marc Rotenberg, EPIC President; and Caitriona Fitzgerald, EPIC Policy Director	8
Letter dated December 4, 2019 to Hon. Roger Wicker and Hon. Maria Cantwell from Scott Talbott, Senior Vice President of Government Affairs, Electronic Transactions Association	11
Statement of Senator Thune	49
Letter dated December 3, 2019 to Hon. Roger Wicker and Hon. Maria Cantwell from Stuart P. Ingis, Counsel, Privacy for America	51
Statement of Senator Blumenthal	52
Statement of Senator Fischer	54
Statement of Senator Schatz	56
Statement of Senator Moran	58
Statement of Senator Markey	60
Statement of Senator Blackburn	62
Statement of Senator Tester	64
Statement of Senator Young	66
Statement of Senator Rosen	67
Statement of Senator Sullivan	70
Statement of Senator Lee	72
Statement of Senator Baldwin	74
Statement of Senator Gardner	79

WITNESSES

Hon. Julie Brill, Corporate Vice President, Deputy General Counsel, and Chief Privacy Officer, Microsoft Corporation	12
Prepared statement	14
Hon. Maureen Ohlhausen, Co-Chair, 21st Century Privacy Coalition	17
Prepared statement	19
Laura Moy, Associate Professor of Law, Georgetown University Law Center; Director, Communications & Technology Law Clinic; and Associate Director, Center on Privacy & Technology	22
Prepared statement	24
Nuala O'Connor, Senior Vice President and Chief Counsel, Digital Citizenship, Walmart Inc.	34
Prepared statement	36
Michelle Richardson, Director, Privacy and Data, Center for Democracy & Technology	40
Prepared statement	42

APPENDIX

Response to written questions submitted to Hon. Julie Brill by:	
Hon. Shelley Moore Capito	83
Hon. Amy Klobuchar	83
Hon. Tom Udall	84
Response to written questions submitted to Hon. Maureen Ohlhausen by:	
Hon. Shelley Moore Capito	85

Page

Response to written questions submitted to Hon. Maureen Ohlhausen by—Continued
Hon. Tom Udall 86
Response to written questions submitted to Laura Moy by:
Hon. Amy Klobuchar 87
Hon. Tom Udall 87
Response to written questions submitted to Nuala O'Connor by:
Hon. Shelley Moore Capito 88
Hon. Tom Udall 89
Response to written questions submitted to Michelle Richardson by:
Hon. Amy Klobuchar 89
Hon. Tom Udall 90

EXAMINING LEGISLATIVE PROPOSALS TO PROTECT CONSUMER DATA PRIVACY

WEDNESDAY, DECEMBER 4, 2019

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

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

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

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

The CHAIRMAN. Good morning. Today the Committee convenes to discuss legislative proposals to protect the privacy of consumer data, both offline and online in the United States. I welcome our distinguished panel of witnesses and thank them for appearing. They include: Ms. Maureen Ohlhausen, former Acting Chair of the Federal Trade Commission and Co-Chair of the 21st Century Privacy Coalition; Ms. Julie Brill, former Commissioner of the Federal Trade Commission; Ms. Nuala O'Connor, Senior Vice President and Chief Counsel of Digital Citizenship at Walmart; Ms. Michelle Richardson, Director of Privacy and Data at the Center for Democracy and Technology; and Ms. Laura Moy, Executive Director and Associate Professor of Law at the Georgetown Law Center on Privacy and Technology.

For the past year, members of this Committee have worked to develop a strong national privacy law that would provide baseline data protection for all Americans. Given the 2018 implementation of the European Union's General Data Protection Regulation, the passage of the California Consumer Privacy Act, and near daily reports of data breaches and misuse, it is clear that Congress needs to act now to provide stronger and more meaningful data protections to consumers and address the privacy risks that threaten the prosperity of the Nation's digital economy. The input of a large number of stakeholders, including consumer advocacy groups, State and local governments, nonprofits, and academia have all been successful in this effort.

Representatives from the private industry such as retailers and convenient stores, software, internet, and cloud service providers, technology companies, small businesses, and several other job cre-

ators in my home state of Mississippi and across the country have also provided thoughtful insights to this Committee. Throughout this process, we have heard many ideas about how best to protect data from misuse and unwanted collecting and processing. These ideas involve providing all Americans with more transparency, choice, and control over their data, as well as ways to keep businesses more accountable to consumers when they seek to use their data for other purposes.

We have heard proposals about how to strengthen the Federal Trade Commission to ensure it has the tools and resources it needs to take swift action against bad actors in the marketplace and effectively respond to changes in potentially harmful technology. That is the FTC's role as the primary enforcement authority over consumer data privacy. An important element of this conversation has been how to achieve each of these goals while preserving the economic and social benefits of data. These benefits not only drive increased productivity, convenience, and cost savings, but they also spur job creation and promote U.S. leadership and technology developments.

Ultimately, to foster continued innovation among our countries entrepreneurs and job creators, Americans need to maintain trust and confidence that their data will be protected and secure. Today marks another step forward in the Committee's efforts to create a national data privacy law. Some of the proposals we will cover today seek to establish consumers' rights and protections over their data in a manner that would provide certainty and clear workable rules of the road for businesses in all 50 states.

This hearing provides an opportunity to hear from expert witnesses on ways to refine these proposals. That should include a discussion on the benefits of creating a strong national and preemptive privacy law that provides consumers with certainty that they will have the same set of meaningful data protections no matter where they are in the United States.

Second, the best way to make sure consumers know about and have a right to opt out of the data collection practices of businesses they deal with. Number three, how requirements on businesses to limit the amount of data they collect and retain about consumers may impact product development and innovation, or what content a consumer is able to view or engage with online. Four, how heightened protections over more sensitive personal data, such as information about financial records and biometric information, would help prevent fraud, identity theft, and security breaches, and whether companies should be required to provide similar heightened protections to non-sensitive data.

Fifth, the merits of creating accountability measures for businesses including requirements to conduct privacy, impact assessments when creating new products and services, and designating data privacy and security officers to oversee ongoing data practices. Six, how empowering consumers with rights over their data and providing additional resources and authorities to the FTC would help strengthen data protections and confidence in the safety and security of the Internet marketplace.

And finally, what enforcement mechanisms are the best way to ensure requirements in a law and see that privacy protections are

enforced. Let me take a moment to acknowledge and thank members of this Committee, up and down the dais on both sides for excellent and thoughtful work during the past year and even before, and who continue as members of the Senate to actively work on legislation that seek to protect consumer privacy.

I appreciate the efforts of each and every member and the valuable contributions the members are making to this important work. And thank you again to our witnesses. This should be a very important hearing and I am delighted now to recognize the Ranking Member, Senator Cantwell, for her opening remarks.

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

Senator CANTWELL. Thank you, Mr. Chairman. It is safe to say this is the other hearing this morning. And not only that, I am glad to see that all the witnesses testifying today are people I know for sure care about privacy. I think it is historic that it is an all-women panel this morning, but again, thanks to each and every one of you trying to advocate on these important issues. Cyber Monday was just a couple of days ago, and it set a record, $9 billion in sales and an increase of 19 percent over last year.

For the first time ever, it was $3 billion that came from people using smartphones to make those purchases. So during the peak hours between 11 p.m. and midnight—I am sorry, 11 p.m. Eastern time and midnight—consumers spent an average of $11 million every minute. So it is not just Cyber Monday that is reminding us, because we all know that we buy groceries, fill prescriptions, pay bills, connect to home devices, to the internet, apply for loans, stay connected with family and friends, and social media, and so much more of our lives are lived online. Which means more information is shared, which means deeply, sometimes personal information is shared. And that information can be used to be targeted or to exclude consumers, to be sold, or even worse, it can be stolen. And that is why we are here today, because we want to protect consumers' privacy rights.

We believe to do that you need strong enforcement and mechanisms to make sure that those rights are protected. The risks that we face online are real. We know that companies today are using ads that might be only for the purposes of targeting what they think is a correct population, young men to work in software, but others can see those ads as discriminatory, or not making themselves available to what information is out there on a job.

Google's Nest camera was involved in an alarming situation where a hacker was able to hack into a couple's baby camera, shouting obscenities before they were able to disable the device. A woman in Portland, Oregon had a private conversation sent by an Alexa device when it went rogue to a colleague.

And then, of course, there is the huge issue of marketed and stolen information, Social Security numbers, login information, drivers' licenses, passports, all now going in the thousands of dollars on the dark web, and in fact in 2005 more than 11 billion consumers have had their information breached. Just last month, the Washington State Attorney General released a report saying that the number of data breaches in my state has increased nearly 20

percent in one year. So that is a matter of our digital footprints continuing to be under attack. It is Congress' job to make sure that Americans are protected and that this information, that is an ever-connected, ever-evolving world, is protected.

And that is why a few weeks ago Senators Schumer, Brown, Murray, Feinstein, and myself joined together to talk about a privacy framework, legislation from all of those committees, that we think would be important for the milestones, the privacy goals that should be met. Last week, Senators Schatz, Klobuchar, Markey, and myself also introduced the Consumer Online Privacy Act that guarantees new rights to consumers and strong enforcement. As the Chairman mentioned, many of our colleagues here, Senator Blumenthal, Senator Thune, Senator Blackburn, and others have been involved in these privacy discussions as well, and we welcome everyone's input on how we move forward.

The important things that we think should be there is that you should have the right to make sure your data is not sold. That you have the right to make sure your data is deleted. That you have the right to make sure that you are not discriminated against with data, and the right to just have plain old transparency about what is being done on a website.

All of these things are tangible and meaningful for consumers. I say they just need to be clear as a bell so that people understand what their rights are and so they know how to enforce them. So today we are here to hear from a group of witnesses who are going to tell us how those issues might be interpreted for the future. But I think the Director of the New York Law School's Innovation Center, Ari Ezra Waldman, recently made a statement that really resonated with me. He said, "we can pass any laws we want, but if there is no way to enforce them, then what is the point?"

So today we also have to talk about enforcement, because enforcement is going to be the key to making sure that privacy rights are actually upheld, that the consumer is truly protected. And if we want the consumers to have that protection, then we also have to make sure that there is accountability, that there are whistleblowers, that there are cases against abuses that might happen. If your privacy rights are violated, you need to be first able to find out about it, and then you need to have the power to do something about it as well, and that is why we think our strong legislation does so. But I also want to say how much this issue is evolving.

Today's *Seattle Times* features a very large announcement by the Knight Foundation and the University of Washington, and Washington State University, on this issue of the public being fooled by online manipulation, whether that is news stories, digital forgeries, or fakes. They want to focus on developing research and tools to resist misinformation, promote an informed society, and strengthen the discourse and discussion in America. I am so proud that these institutions are taking on this challenge, and that this kind of national initiative in our legislation, with NIST, the National Institute of Standards and Technology, at the Department of Commerce, would be empowered in the legislation we introduce to help with this effort.

While we are here today to talk about just some basics in digital hygiene online, the future though is this, the challenges we face as

more and more misinformation, forgery, things we can't even detect whether they are true or not, will continue to appear online. We need to build a strong system today in a Federal framework that will help us continue to grow for the ever-changing technology future. That is what we are dedicated to.

I look forward to hearing the witnesses today and seeing how we can move forward in this important policy area. Thank you, Mr. Chairman—and if I could also just enter into the record, a list of organizations, a letter sent to you and I, of organizations sponsoring, supporting privacy legislation. And I will just mention a few others if I could, Mr. Chairman.

The CHAIRMAN. Without objection. That will be entered into the record at this point.

[The information referred to follows:]

CONSUMER BANKERS ASSOCIATION
Washington, DC, December 3, 2019

Hon. ROGER WICKER, Chairman,
U.S. Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Hon. MARIA CANTWELL, Ranking
Member,
U.S. Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Dear Chairman Wicker and Ranking Member Cantwell:

On behalf of the Consumer Bankers Association (CBA), I write to share our views on a national data privacy framework for the Senate Commerce, Science and Transportation Committee's hearing entitled "Examining Legislative Proposals to Protect Consumer Data Privacy." CBA is the voice of the retail banking industry whose products and services provide access to credit for consumers and small businesses. Our members operate in all 50 states, serve more than 150 million Americans, and collectively hold two-thirds of the country's total depository assets.

The State of Data Privacy

Unfortunately, data breaches have become all too prevalent in our digital world and consumers are rightly concerned about the manner in which their personal information is collected, shared, protected and stored. In 2018 alone, the number of data breaches in the U.S. totaled more than 1,200 according to the Identity Theft Resource Center. No industry was immune from breaches in 2018: business sector (46 percent), healthcare/medical industry (29 percent), banking/credit/financial industry (11 percent), government/military (8 percent), and the education sector (6 percent). When taking a closer look at the data it is clear, the non-financial business sector, which is not subject to national data security requirements, was responsible for the overwhelming majority (93 percent) of the personal records compromised. In addition to breaches, concerns regarding the misuse of customer data warrant a review of industry practices and the scope of Federal privacy laws and regulations, *e.g.,* Cambridge Analytica gained access to private information on more than 50 million Facebook users.[1]

CBA members take seriously their responsibility to clearly explain how consumer data is used and to safeguard it against improper use and criminals' nearly constant attempts to steal it. Since the passage of the Gramm-Leach-Bliley Act (GLBA) in 1999, financial institutions have been required to provide their customers a clear privacy notice detailing information collection and sharing practices, which includes an opt-out for the sharing of information with non-affiliated third parties. This notice is provided at the beginning of the customer relationship and annually thereafter. GLBA and subsequent regulations also require banks to have in place data security protocols to safeguard sensitive consumer information and to report to Federal authorities and affected consumers when a breach occurs. Banks are examined by their prudential regulators on these standards and if found to be non-compliant may face fines or other penalties.

The low breach-rate of personally identifiable information (PII) at financial institutions compared to other sectors can be attributed to the common-sense safeguards

[1] *https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html*

required by GLBA and the industry's commitment to security. As a result, consumers trust financial institutions more than any other type of organization to keep their financial information secure, according to an August 2017 poll by Morning Consult.

Consumer Privacy

Consumers should have reasonable control concerning the collection, use and sharing of personal data. However, we caution against national privacy legislation that may inhibit banks' ability to fulfill their contractual obligations to consumers. Compared to other industries, banks are subject to more stringent rules and lead in protecting consumers' PII and their privacy.

Pursuant to the GLBA, banks are required to protect the security and confidentiality of consumer records and information, and the law also requires banks to disclose their privacy practices and limits sharing PII with nonaffiliated third parties. Any Federal privacy law must consider the GLBA and other existing Federal privacy laws and preempt the growing patchwork of state laws that provide differing and inconsistent consumer protections. Otherwise, a consumer's privacy protections, including their ability to understand their rights, will depend on the state where the individual resides. While these state laws may be well-intentioned, they must be crafted to not hinder the free flow of data needed to provide consumers and businesses with financial products and services and process financial transactions.

As Congress considers the creation of a national data privacy framework, we must first recognize the differences in data collection among industries. Banks are required by Federal law to collect certain information to conduct a customer transaction. For example, if a consumer wants to open a checking account, at a minimum pursuant to the Bank Secrecy Act, the bank must obtain certain information to fulfill its Customer Identification Program requirements, such as date of birth, address, and identification number. As an additional benefit to customers, banks also use personal data to develop banking products and services that are customized to a customer's needs. Utilizing consumer data to conduct financial transactions authorized by the consumer is far different than a social media platform collecting consumer data to sell to marketers.

It is also important that a Federal privacy standard should not unnecessarily expand the scope of data that banks are responsible for protecting. GLBA requires banks to protect consumers "nonpublic personal information", which is defined, in part, as "[. . .] personally identifiable financial information, (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[2] Consumer is defined to mean "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative."[3] An expansion of the definition of covered data or covered persons pursuant to a national standard would subject banks to unnecessary and costly regulatory burden without any additional benefit to consumers.

A national data protection and privacy law must seek to promote innovation, investment and competition in the marketplace. The United States Constitution authorizes Congress to regulate interstate commerce, which includes the free flow of goods and consumer data. A patchwork of privacy laws at the state level will lead to higher costs for consumers and create barriers to innovation and investment. The assumption that preemption weakens existing state laws is a misconception of today's digital marketplace. In a world that is increasingly mobile, Americans and their devices constantly cross state borders. Consumer protection should not depend upon which state you reside, but consumers should be covered by one unified, comprehensive Federal standard.

From an international perspective, CBA also supports an open global economy that enables growth through the secure and efficient transfer of data across international borders. National data protection and privacy legislation should continue to support consumer privacy while also respecting and coordinating differences between U.S. and foreign privacy regimes.

National data protection and privacy legislation should be enforced by the Federal Trade Commission (FTC), unless a determination is made that it is appropriate for a different regulator to be the enforcement agency, *e.g.,* prudential regulators for banks and credit unions. CBA is concerned that if 50 state attorney generals bring

---

[2] *https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=15-USC-697127498-1137964384&term_occur=2&term_src=title:15:chapter:94:subchapter:I:section:6801*

[3] *https://www.law.cornell.edu/uscode/text/15/6809#4_A*

enforcement actions in Federal court, there is a high probability each state will enforce the law differently, inviting confusion, complexity and increased compliance burden. In addition, a national consumer privacy law should not provide for a private right of action.

Data Security and Breach Notification

It is also critical that any conversation around data privacy also take seriously the security of data and the protocol for notifying customers in the event of a breach for *all* who operate within the payments system. Banks are on the front lines, investing large amounts of operating capital in fraud monitoring and security. Our member institutions consistently monitor our customer accounts for fraud and work to make consumers whole, no matter where a breach occurs. Consumers rely on their financial institutions to communicate what to do in the event of a breach and to employ defenses to prevent fraud and identity theft.

Subsequent to Section 501(b) of GLBA, the financial regulators issued guidelines requiring banks to implement comprehensive, risk-based information security programs that include administrative, technical and physical safeguards to protect customer information. These safeguards are not static but flexible and scalable—applying to banks of all sizes. A similar framework should be applied to non-bank companies to ensure consumers' sensitive information is protected throughout the payment system.

Banks must also implement a risk-based response program in the event of a breach. The program includes an evaluation of the incident and an effort to prevent further unauthorized access as well as notice to the institution's primary Federal regulator, appropriate law enforcement, and importantly, the customers whose information was breached and could be misused. CBA supports and urges Congress to consider passing legislation that will require others in the payment system to provide timely notification to their customers in the event of a breach.

Today, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of a security breach of information involving PII.[4] Twenty-four states currently have data security laws requiring a level of security procedures and practices to be in place to protect personal information.[5]

Congress has the constitutional authority to regulate interstate commerce through the Commerce Clause, which was written to prevent fragmentation of markets and to encourage the free flow of goods and services, including information, across the Nation with minimal interference. Congress should take seriously its authority and enact a Federal data security and breach notification standard and preempt the current patchwork of state laws. Breaches put consumers at risk and the urgent need for a national standard that will ensure all who operate within the payments system employ the strongest safeguards could not be more evident as more Americans prefer the ease of the electronic payment system to purchase goods and services. Protecting consumer information is a shared responsibility of all parties involved.

Lessons from the California Privacy Protection Act

Lastly, the California Consumer Privacy Act ("CCPA") is the first major consumer privacy law to be adopted at the state level. This legislation was written hastily, and the California Attorney General is currently reviewing and revising portions of the law through its regulatory process. As the California privacy law continues to evolve, it would be prudent for Congress to monitor issues with implementation and use observations from industry stakeholders to draft a Federal data privacy and security standard.

In general, CBA member banks support providing consumers with an expanded set of consumer privacy rights. However, the CCPA as currently written has some critical flaws which will harm both consumers and businesses. For example, the proposed regulations require a bank to specify a concerning level of detail about certain privacy practices, which could potentially benefit social engineers looking to commit fraud. According to a whitepaper published by Blackhat USA 2019, which considers the legal ambiguity surrounding the European Union's General Data Protection Regulation's "Right of Access" process, ". . .[L]egislators can weaken many of the factors which encourage businesses to improperly implement identity verification. Simply assuring businesses that rejecting a suspicious right of access request in good faith will not later result in prosecution if it turns out that the request origi-

---

[4] *http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*

[5] *http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx*

nated from a legitimate but suspiciously-behaving data subject may be all that's needed. . .".[6]

Other concerns with the CCPA include the definition of "sell" and its impact on service providers, as well as the lack of reasonable limitations on consumer privacy rights to protect intellectual property and avoid infringement issues. Considering the importance of this issue and the impact it will have on both consumers and businesses, it is imperative that Congress is thoughtful in drafting meaningful legislation to protect consumers and provide businesses with certainty.

On behalf of our members, I would like to thank you for your consideration of our views. We look forward to working with the Committee to foster an environment that prioritizes the protection and privacy of consumer data while promoting consumer access to credit.

Sincerely,

RICHARD HUNT,
President and CEO,
Consumer Bankers Association.

ELECTRONIC PRIVACY INFORMATION CENTER
Washington, DC, December 3, 2019

Hon. ROGER WICKER, Chairman,
Hon. MARIA CANTWELL, Ranking Member,
U.S. Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Chairman Wicker and Ranking Member Cantwell:

We write to you in regarding your hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy."[1] EPIC appreciates the Committee's focus on data privacy. The time is past due for Congress to act on privacy. Congress' failure to pass comprehensive baseline privacy legislation or to establish a U.S. Data Protection Agency has put Americans' personal data at risk.

The U.S. is one of the few developed countries in the world without a data protection agency. The practical consequence is that the U.S consumers experience the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber-attack by criminals and foreign adversaries. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security.

EPIC warned the Senate about foreign access to consumer data over two years ago. In testimony before the Senate Banking Committee, EPIC President Marc Rotenberg said:

> U.S. consumers, businesses, and the U.S. government face a genuine threat from the unbounded collection of personal data without adequate legal and technical protections. This data is now the target of foreign adversaries. Two years ago it was the OPM breach. Now it is the Equifax breach. I am reluctant to imagine the consequences for the United States of the next major breach.[2]

But Congress has taken no action.

The United States Needs a Data Protection Agency

There is an urgent need for leadership from the United States on data protection. Virtually every other advanced economy has recognized the need for an independent agency to address the challenges of the digital age. Current law and regulatory oversight in the United States is woefully inadequate to meet the challenges. In 2011, following the Facebook and Google consent orders, EPIC believed that the FTC could function as an effective privacy agency but that is clearly no longer true. Even FTC Commissioner Joe Simons recently conceded in a Congressional hearing that

---

[6] *https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf*

[1] *Examining Legislative Proposals to Protect Consumer Data Privacy,* S. Comm. on Commerce, Sc., and Trans. (Dec. 4, 2019), *https://welcome/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy.*

[2] *Hearing on Consumer Data Security and the Credit Bureaus,* S. Committee on Banking, Housing, and Urban Affairs (Testimony of Marc Rotenberg, President, EPIC) (Oct. 17, 2017), *https://epic.org/testimony/congress/EPIC-Testimony-SBC-10-17.pdf.*

the FTC does not have the authority to safeguard privacy.[3] *The United States urgently needs a Data Protection Agency.*

The FTC is ineffective. The agency ignores most complaints it receives, does not impose fines on companies that violate privacy, and is unwilling to impose meaningful penalties on repeat offenders.[4] In documents obtained in September 2019 by EPIC, we uncovered 3,000 complaints new complaints filed with the FTC *since the Commission proposed the $5 billion settlement with Facebook two months ago.*[5]

Earlier this year, our case EPIC v. FTC determined that there were over 26,000 complaints against Facebook pending with the Commission.[6] *The FTC is simply ignoring thousands of consumer privacy complaints about Facebook's ongoing business practices.* The Federal Trade Commission may help consumers with broken toasters, but the FTC is not an effective data protection agency. Even when the FTC reaches a consent agreement with a company, the Commission fails to protect the interests of consumers.[7]

The FTC Chairman has made much of the large fines recently imposed against Facebook and Google. But large fines are not the solution to data protection. EPIC, Color of Change, the Open Markets Institute and others wrote to the FTC in January telling the agency that more than fines are necessary in the Facebook case.[8] Our groups called for equitable remedies, including reforming hiring and management practices at Facebook. *EPIC called for the FTC to require Facebook to unwind the acquisition of both WhatsApp and Instagram,*[9] a view that is now widely shared by many experts in the antitrust field. Our groups also recommended that the FTC require Facebook to add an independent director who represents the interest of users and also examine the civil rights impacts of Facebook's products and policies.

The 2011 Facebook Order was the result of an extensive complaint filed by EPIC and a coalition of consumer organizations in 2009, following Facebook's repeated changes to its privacy settings that overrode user preferences and allowed third parties to access private information without users' consent.[10] The FTC has an obligation to the American public to ensure that companies comply with existing Consent Orders. It is unconscionable that the FTC allowed this unprecedented disclosure of Americans' personal data to occur. *The FTC's failure to act imperils not only privacy but democracy as well.*

For many years, FTC Chairmen and Commissioners assured Congress and representatives of the European governments, responsible for safeguarding European consumers, that the FTC was an effective privacy agency.[11] One former FTC Chair-

---

[3] *Online Platforms and Market Power, Part 4: Perspectives of the Antitrust Agencies,* 116th Cong. (2019), H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial, and Administrative Law, *https://judiciary.house.gov/legislation/hearings/online-platforms-and-market-power-part-4-perspectives-antitrust-agencies* (testimony of Joseph Simons, Chairman, Fed. Trade Comm'n at 1:35:45: "on the privacy side, we have one hundred year old statute that was not in any way designed or anticipating the privacy issues that we face today.") (Nov. 13, 2019).

[4] Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.,* FTC File No. 1823109 at 17 (July 24, 2019), *https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.*

[5] EPIC, *EPIC Uncovers 3,156 More Facebook Complaints at FTC—Over 29,000 Now Pending* (Sept. 22, 2019), *https://epic.org/2019/09/epic-uncovers-3156-more-facebo.html.*

[6] EPIC, *EPIC FOIA—FTC Confirms More than 25,000 Facebook Complaints are Pending* (Mar. 27, 2019), *https://epic.org/2019/03/epic-foia—ftc-confirms-more-.html.*

[7] *See EPIC v. FTC,* No. 12–206 (D.C. Cir. Feb. 8, 2012).

[8] Letter from EPIC *et al.,* to Joseph Simons, Chairman, Federal Trade Comm'n (Jan. 24, 2019), *https://epic.org/privacy/facebook/2011-consent-order/US-NGOs-to-FTC-re-FB-Jan-2019.pdf.*

[9] *See* Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* 132–33 (2018).

[10] EPIC, et al, In the Matter of Facebook, Inc. (Complaint, Request for Investigation, Injunction, and Other Relief) (Dec. 17, 2009), *https://epic.org/privacy/inrefacebook/EPIC-Facebook Complaint.pdf.*

[11] According to the statement of the FTC Commissioners who testified before the Senate Commerce Committee in 2012:

> Similar to the Google order, the Commission's consent order against Facebook prohibits the company from deceiving consumers with regard to privacy; requires it to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user's information after she deletes that information.

The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission: Hearing Before the S. Comm on Commerce, Science and Transportation, at 18, 112th Cong. (May 9, 2012) (statement of Fed. Trade Comm'n.), HTTPS://WWW.FTC.GOV/SITES/DEFAULT/FILES/DOCUMENTS/PUBLIC_*statements/prepared-statement-federal-trade-commission-need-*

Continued

man even proposed that the FCC's privacy jurisdiction be transferred to the FTC because the FTC was doing such an incredible job.[12]

The FTC's problems are not lack of budget or staff. The FTC has not even filled the current post for a Chief Technologist. The FTC has simply failed to use its current resources and current authorities to safeguard consumers.

Given the enormity of the challenge, the United States would be best served to do what other democratic countries have done and create a dedicated Data Protection Agency, based on a legal framework that requires compliance with baseline data protection obligations.[13] An independent agency could more effectively police the widespread exploitation of consumers' personal data and would be staffed with personnel who possess the requisite expertise to regulate the field of data security.[14]

EPIC encourages Congress to update U.S. privacy law and to create a Data Protection Agency. EPIC's new report *Grading on a Curve* also sets out the key elements of a comprehensive privacy law.[15] As you consider data privacy legislation, we urge you to review EPIC's report, attached to this statement.

We ask that this letter and the attachments be entered in the hearing record.

Sincerely,

MARC ROTENBERG	CAITRIONA FITZGERALD
Marc Rotenberg	Caitriona Fitzgerald
EPIC President	EPIC Policy Director

Attachments

EPIC, *Grading On A Curve* (2019).

Marc Rotenberg, *America Needs a Privacy Law,* New York Times (December 25, 2018)

Marc Rotenberg, *Congress can follow the EU's lead and update U.S. privacy laws,* Financial Times (June 1, 2018) ("Regarding innovation, it would be a critical mistake to assume that there a trade-off between invention and privacy protection. With more and more devices connected to the Internet, privacy and security have become paramount concerns. Properly understood, new privacy laws should spur the development of techniques that minimize the collection of personal data.")

---

privacy-protections-perspectives-administration-and/120509privacyprotections.pdf; see also, The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Hearing before the S. Comm. on Commerce, Science, and Transportation, 112th Cong. (May 19, 2012) (statement of Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n) ("We have also charged companies with failing to live up to their privacy promises, as in the highly publicized privacy cases against companies such as Google and Facebook, which together will protect the privacy of more than one billion users worldwide. As a Commissioner, I will urge continuation of this strong enforcement record."), *https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120509privacytestimony.pdf;* Letter from FTC Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission, at 4–5 (Jul. 7, 2016), *https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v.*

[12] Jon Leibowitz and Jonathan Nuechterlein, *The New Privacy Cop Patrolling the Internet* (May 10, 2016), *http://fortune.com/2016/05/10/fcc-internet-privacy/.*

[13] EPIC, *The U.S. Urgently Needs a Data Protection Agency,* https://epic.org/dpa/; *also see* attached.

[14] *See* Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States* (2019), *https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf.*

[15] *See https://epic.org/GradingOnACurve/.*

ELECTRONIC TRANSACTIONS ASSOCIATION
Washington, DC, December 4, 2019

Hon. ROGER WICKER,
Chairman,
Committee on Commerce, Science, and Transportation,
United States Senate,
Washington, DC.

Hon. MARIA CANTWELL,
Ranking Member,
Committee on Commerce, Science, and Transportation,
United States Senate,
Washington, DC.

Dear Chairman Wicker, Ranking Member Cantwell, and Members of the Committee:

The Electronic Transactions Association ("ETA") appreciates the opportunity to submit this statement for the record before the Committees hearing, "Examining Legislative Proposals to Protect Consumer Data Privacy."

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions, mobile payment service providers, mobile wallet providers, and non-bank online lenders that make commercial loans, primarily to small businesses, either directly or in partnership with other lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient, and rewarding payment solutions and lending alternatives.

ETA and its members support U.S. and international efforts to strengthen privacy laws in ways that help the 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 the government coordinates 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.

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 U.S. 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 framework should include the following principles:

- *National Standard*
  By providing consumers and businesses with consistent protections through an established, uniformed law, consumers and businesses will benefit. Enacting a Federal uniform national standard will provide certainty and consistency to businesses and consumers alike without having to navigate the patchwork of state laws. A uniform national standard—that is the ceiling—would also reduce the complexity and costs associated with the compliance and enforcement issues resulting from a patchwork of laws.
- *Permissible Uses*
  The payment industry has a long commitment and history of fighting fraud and 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.
- *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.

- *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 Federal Trade Commission ("FTC") and state attorneys general to enforce a national consumer privacy law. Strict coordination should be followed to avoid duplicate or conflicting enforcement actions. ETA believes the FTC should be granted targeted rulemaking authority and have civil penalty authority. However, a Federal privacy law should not provide monetary relief in the form of 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.
- *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. The U.S. is uniquely positioned to benefit from the experience and regulatory proposals being adopted or considered by its international counterparts. But having the U.S. 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 participants 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 Committee for this opportunity to provide this statement for the record on this important topic and 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.

The CHAIRMAN. And we are now delighted to hear from our panel, and we will simply begin at this end and move down the table. Ms. Brill, you are recognized.

STATEMENT OF HON. JULIE BRILL, CORPORATE VICE PRESIDENT, DEPUTY GENERAL COUNSEL, AND CHIEF PRIVACY OFFICER, MICROSOFT CORPORATION

Ms. BRILL. Thank you so much. Chairman Wicker, Ranking Member Cantwell, members of the Committee, thank you for this opportunity to testify about the urgent need for comprehensive national privacy legislation. It is a privilege to be here. My name is Julie Brill. I am Microsoft's Corporate Vice President, Deputy General Counsel, and Chief Privacy Officer. I joined Microsoft two years ago after more than 25 years of public service dedicated to consumer protection, competition, and privacy enforcement, includ-

ing six years as Commissioner of the U.S. Federal Trade Commission.

I want to thank all of you for your work to address the privacy concerns of the American people. Your proposals recognize that too much of the responsibility for protecting privacy in our digital world falls on individuals. Like many of you, Microsoft believes that consumers should no longer bear the sole responsibility and the sole burden for privacy protection. Instead, we believe that consumers should have the right to control their own data for sure and that companies should be responsible and accountable for the data they collect and the way they use it.

As you know, we live in a remarkable technology driven world in an era of change. Over the past few years, cloud computing has transformed how we work, how we play, and how we connect with one another. Entire industries have been reinvented and this is just the beginning. Now rapid advances in artificial intelligence are providing unprecedented opportunities to create a stronger economy and a healthier and more prosperous world. These opportunities are built on the ability to collect and analyze data at a scale that has never been possible before.

Some of this data is deeply personal information about our health, our jobs, what we believe, where we go, what we buy, and so much more. This has profound implications for privacy, implications that we have yet to grapple with in this country. Privacy is a basic human right and the foundation from which all other rights flow, including the rule of law and all of our civil liberties. Privacy is also the foundation for consumer trust, which will ultimately determine whether we realize the promise and reap the benefits of these revolutionary data-driven opportunities and capabilities. But today in this country consumer trust hangs in the balance. Under our current laws, the burden on individuals to protect information is simply too great.

As individuals we lack the information we need to understand who is using our data and why. The tools to manage personal information are often too complex. As a result, 4 out of 5 Americans say they have little or no control over the data that companies collect about them, 4 out of 5 Americans are concerned about how their personal data is used, and 4 out of 5 Americans believe that the risks from all of this data collection outweigh the benefits. The California Consumer Privacy Act of 2018 was a significant step toward addressing these concerns.

Now, the time has come for Congress to act. The imperative to enact strong Federal privacy protections within a framework that enables American innovation to thrive has never been greater. At Microsoft we believe privacy legislation should reflect four key principles. First, transparency about how companies collect, use, and share personal information.

Second, consumer empowerment that guarantees the right of individuals to access, correct, delete, and move their personal information to another provider. Third, corporate responsibility that requires companies to be good stewards of consumer information. And finally strong enforcement through a central regulator like the FTC that has the necessary authority and funding, and through State Attorneys General.

We urge members of this Committee to come to a bipartisan consensus so that American consumers enjoy the privacy protections that so many others around the world already have and that are so long overdue in this country. Thank you.

[The prepared statement of Ms. Brill follows:]

PREPARED STATEMENT OF JULIE BRILL, CORPORATE VICE PRESIDENT, DEPUTY GENERAL COUNSEL, AND CHIEF PRIVACY OFFICER, MICROSOFT CORPORATION

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to share Microsoft's views on the need for comprehensive Federal privacy legislation.

My name is Julie Brill. I am Microsoft's Corporate Vice President, Deputy General Counsel, and Chief Privacy Officer. I joined Microsoft after a long career in public service dedicated to consumer protection, competition and privacy, including six years as a Commissioner of the U.S. Federal Trade Commission ("FTC") and more than 20 years working at the state level in roles including Chief of Consumer Protection and Antitrust for the States of North Carolina and Vermont and head of the Privacy Working Group of the National Association of State Attorneys General.

Microsoft has provided me a unique opportunity to continue contributing to the future of privacy and consumer protection, because it is both a world leader in creating the technologies that are transforming people's lives and in the responsible and transparent use of personal information. During my time at the company, I have met with regulators and customers around the world, and it is clear from these meetings that the time for strong privacy legislation is now.

America Deserves a Comprehensive Privacy Law

We live in a time of remarkable technology-driven change and disruption. How people work, play, shop, and learn about the world has been transformed over the last decade. Industries have been reinvented. New ways to diagnose and treat diseases have emerged. And the way people connect with one another has been reimagined.

Groundbreaking technologies have driven these changes. Cloud computing—which enables governments, companies, and individuals to analyze and derive insights from data at a scale previously not possible—is now the norm, and it is clear that the progress made thus far is only the beginning. For example, the rapid emergence of artificial intelligence and machine learning technologies holds great promise for the future, as does the rise in quantum computing.

These technologies unquestionably will be transformative and impact our daily lives. Even more so than today, they will raise questions about how we protect the privacy of personal information.

Accompanying these technological changes is a global movement to adopt sweeping legal frameworks to enhance consumer privacy and protect personal information. Europe enacted a landmark data protection law that has been in effect since May 2018: the General Data Protection Regulation ("GDPR").[1] New privacy laws have also recently passed or are currently being developed in Brazil, China, India, Japan, Kenya, and Thailand.[2] Each of these legal regimes include some common principles for data protection. And, together, they are defining global baselines for privacy protection.

In the United States, California has enacted the California Consumer Privacy Act of 2018 ("CCPA"), which takes effect this coming January.[3] The CCPA was the first comprehensive privacy law to be passed in the United States. Its provisions reflect emerging international norms, including rights for consumers to access and delete their personal information. Other U.S. states are considering new comprehensive privacy laws as well.[4]

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing 95/46/EC (General Data Protection Regulation).

[2] *See* Brazilian Internet Law, Law. No. 13,709 of August 14, 2018; China GB/T 35273–2017 Information Technology—Personal Information Security Specification (effective May 1, 2018); India Personal Data Protection Act, 2018 (draft bill); Japan Amended Act on the Protection of Personal Information (effective May 30, 2017); Kenya Data Protection Act, 2018 (draft bill); Thailand Draft Personal Data Protection Act, B.E. 2562 (effective May 27, 2019).

[3] Cal. Civ. Code § 1798.100 *et seq.*

[4] *See, e.g.,* Washington SB 5376 (introduced Jan. 18, 2019); Minnesota HF 2917 (introduced May 19, 2019).

These state-level efforts are important, as they demonstrate the need for comprehensive privacy laws in the United States. U.S. privacy law has generally failed to keep pace with advances in technology and to provide Americans with the protections they want and need in this digital age. Unlike Europeans, or Brazilians, or Chinese nationals, Americans today do not enjoy comprehensive privacy protections that apply across the country. As a result, 81 percent of Americans have reported in a Pew Research Center study released last month that they feel they have little or no control over the data collected about them and believe that the potential risks they face from companies' collection of their data outweigh the benefits.[5] Nearly the same percentage of Americans reported that they were concerned about the way their data is being used by companies.

Today more than ever, there is an urgent need for a comprehensive U.S. privacy law that provides strong protections for all consumers in the United States within a framework that enables human ingenuity and American innovation to continue to thrive. Americans need a comprehensive privacy law because, all too often, they do not have sufficient information about who has access to their personal information, who is using it, and for what purposes. In many cases, the privacy tools currently available to American consumers to exercise choices with respect to their personal information are too complex and place unreasonable burdens on people to utilize them.

At the same time, in light of Cambridge Analytica, the Equifax data breach, and other recent revelations, Americans are also concerned about whether companies are held to sufficiently high standards regarding the protection of personal information, and whether companies are appropriately held to account when failing to live up to those standards. The Pew Research Center study I cited above found that most Americans believe their personal information is *less* secure today than in the past, and have little or no confidence in companies' public accountability with respect to misuse or compromise of their personal information. Given these findings, it is no surprise that the same study found that a majority of Americans—regardless of political affiliation—strongly favor increased government regulation of companies' use of their personal information.

Microsoft's Longstanding Commitment to Privacy

At Microsoft, we believe that privacy is a fundamental human right and that, with recent advances in technology, the protection of this right has become more important and more urgent than ever before. Privacy is also the foundation of consumer *trust,* which is crucial to realize the promise of advanced data-driven technologies. We know that people will only use technology when they trust that it will keep their personal information safe and secure, and that companies will collect and use consumers' data in ways that are responsible and demonstrate that they are worthy stewards of that data.

Microsoft has continued to put these principles into practice every day through ongoing investments in tools that give consumers greater control over their personal information and greater visibility into how we handle that information. To date, for example, more than 28 million people globally—including more than 10 million Americans—have used our privacy dashboard to better understand and control their personal information. And we have developed a range of products and services that enable our enterprise customers to comply with their data protection obligations and safeguard their users' information as well.[6]

In addition to our privacy-based innovations, Microsoft has long supported and advocated for strong legal frameworks to protect privacy in the United States and around the world. We have been a proponent of comprehensive Federal privacy legislation in the United States since 2005.[7] We were also early supporters of the GDPR, and in May 2018 we announced that we would voluntarily extend the rights that are at the heart of the GDPR to all of our customers worldwide.[8] These rights

---

[5] Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* (Nov. 15, 2019), *https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information.*

[6] Microsoft Trust Center GDPR Overview, *https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview.*

[7] Microsoft Corp., *Microsoft Advocates Comprehensive Federal Privacy Legislation* (Nov. 3, 2005), *https://news.microsoft.com/2005/11/03/microsoft-advocates-comprehensive-federal-privacy-legislation.*

[8] Julie Brill, *Microsoft's commitment to GDPR, privacy and putting customers in control of their own data* (May 21, 2018), *https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data.*

include the right to know about the data we collect about consumers, to access and correct that data, to delete it, and even to take it to another service if they choose. And just last month, we announced that we would honor the CCPA's core user control rights for consumers throughout the United States, rather than affording them only to California residents.[9]

Microsoft welcomes strong privacy laws like the CCPA in California, in addition to similarly comprehensive privacy laws being considered in other states. The efforts in California and other states have served as important catalysts toward the strong Federal privacy law that our country requires and deserves.

Congress should be inspired to build upon these state-led efforts. In addition to granting American consumers the right to control their personal information and establishing strong mechanisms to enforce compliance, we believe that privacy laws should go further by placing more obligations on companies to become responsible stewards of personal information. These accountability requirements should include enhanced transparency about the purposes for which companies collect and use personal information, an obligation to collect and use only the data reasonably necessary for those purposes, and greater responsibility to analyze and improve internal systems to ensure that companies are using personal information appropriately and in line with reasonable consumer expectations. And companies should have affirmative duties to reasonably secure personal information from unauthorized access and to avoid unlawful discrimination in violation of Federal and state laws.

Necessary Components for a Strong Federal Privacy Framework

Microsoft believes that comprehensive Federal privacy legislation should adhere to four key principles: transparency, consumer empowerment, corporate responsibility, and strong enforcement.

Transparency. Transparency is a centerpiece of virtually all data privacy laws existing today. American consumers should have the right to be informed, in a concise and understandable manner, about what personal information companies collect about them, and how that information is used and shared. Companies should provide this information in a context-appropriate fashion at the most meaningful times during the consumer's experience.

Consumer Empowerment. User control is also a central feature of strong privacy laws. American consumers should be empowered to control their personal information and to express their privacy choices in accordance with rapidly-emerging global norms. In particular, consumers should have rights to access, correct, and delete their personal information, and to move their data to other providers.

In addition, Microsoft believes that Federal privacy legislation should specifically regulate practices that consumers do not expect and that have a particularly high impact on consumer privacy, such as the collection and sharing of personal information by data brokers that operate behind the scenes, and are unknown to consumers. To ensure that consumers can meaningfully exercise their privacy rights with respect to data brokers, Federal privacy legislation should build on concepts from the data broker laws enacted by Vermont and California.[10] The Federal law should require data brokers to register with the Federal regulator, and to provide information about the kinds of data they collect and sell, the location of the consumers whose information is affected, and details about how consumers can exercise their data control rights.

Corporate Responsibility. Companies should act as responsible stewards of consumers' personal information, and should be accountable for their actions. This should include affirmative obligations for companies to minimize the amount of personal information they collect—limiting it to the data that is reasonably necessary for the purposes of collection—and to apply technical and other measures to protect that information. Companies also should be required to analyze and improve their internal systems to ensure that they are using consumer data appropriately and in accordance with reasonable consumer expectations, and to document and make these assessments available to an oversight authority upon request. Ultimately, the higher the risk inherent in the proposed use of data, the greater a company's responsibility should be to protect that data. And, as noted above, companies should have affirmative duties to reasonably secure personal information from unauthorized access, and to guard against unlawful discrimination in violation of Federal and state laws.

---

[9] Julie Brill, *Microsoft will honor California's new privacy rights throughout the United States* (Nov. 11, 2019), *https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights.*

[10] Vt. Stat. Ann. tit. 9, §§ 2446–2447; Cal. Civ. Code § 1798.99.80 *et seq.*

Strong Enforcement. Congress should empower a strong central regulator, such as the FTC, to issue rules and to appropriately enforce the Federal privacy law, and should provide the regulator with sufficient authority, technical capability, and funding to do so. This will help to ensure that the regulatory agency has sufficient capacity and expertise to engage in robust enforcement across the many diverse companies and industries that will be in scope.

A strong Federal law should also empower the State Attorneys General to enforce the provisions of the law.

Conclusion

Microsoft appreciates the desirability of diverse proposals, which will lead to more robust discussion and debate about this critically important issue. We particularly appreciate the bills and discussion drafts that have been released by members of this Committee and others. These proposals represent positive steps in the right direction toward a comprehensive Federal privacy law.

Since 2005, Microsoft has partnered with members of this Committee to advocate for robust consumer privacy protections, and we are eager to continue to do so. We very much appreciate the good work of Chairman Wicker, Ranking Member Cantwell, and other members of the Committee, and look forward to that work continuing apace.

We urge the members of this Committee to come to a consensus that will allow all American consumers to enjoy the privacy protections that so many others around the world already have.

We are optimistic that Congress will pass comprehensive Federal privacy legislation in the very near future, building on the important milestones contained in the CCPA and other state laws. It is past time for the United States to pass meaningful privacy laws that apply to American consumers regardless of where they live in this country. We call on all relevant stakeholders—lawmakers, consumer advocates, industry, government, academics, and others—to join us in working to pass meaningful privacy protections here in the United States. This is an issue worth fighting for.

The CHAIRMAN. Thank you, Ms. Brill. Precisely five minutes. Ms. Ohlhausen.

STATEMENT OF HON. MAUREEN K. OHLHAUSEN, CO-CHAIR, 21ST CENTURY PRIVACY COALITION

Ms. OHLHAUSEN. Thank you. Chairman Wicker, Ranking Member Cantwell, and other distinguished members of the Committee, thank you for the opportunity to testify at this important hearing examining legislative proposals to protect consumer privacy. I am Maureen Ohlhausen, a Partner at the law firm of Baker Botts and the Co-Chair of the 21st Century Privacy Coalition which represents the Nation's leading communications providers and their trade associations.

I also served as a Commissioner and Acting Chairman of the Federal Trade Commission ("FTC"), our Nation's leading consumer privacy agency. But as the collection, use, and sharing of personal data has continued to grow, the FTC is reaching the limit of its current tools, and consumers and businesses are increasingly required to navigate a tangle of confusing and often inconsistent privacy requirements from various levels of Government. We commend the Committee for your leadership and express our support for legislation that will provide transparency and control to consumers, robust security, and strong accountability as outlined in the FTC's 2012 Bipartisan Privacy Report.

We therefore encourage Congress to enact Federal privacy legislation that includes three key attributes. First, it should provide consumers clarity and visibility into companies' data collection, use, and sharing practices as well as choices regarding these practices calibrated to the sensitivity of that data. Second, legislation should

provide a national and uniform set of protections and consumer rights throughout our digital economy. Third, it should ensure strong enforcement that protects consumers from harmful data practices while allowing companies to provide innovative products and services that consumers want.

Let me elaborate on those three points briefly. First, an optimal approach would balance ease-of-use and transparency by giving consumers clear and simple privacy choices based on the nature of the relevant information itself, its sensitivity, and its risk of consumer harm if such information is misused. Sensitive, personal information such as health and financial information, real-time geolocation information, and Social Security numbers should be subject to the highest protections.

In turn, to reflect consumer expectations and preferences, there should be less stringent requirements on non-sensitive personal information as well as on information that is de-identified or aggregated because such information has a lower risk of consumer harm. And for certain types of routine operational uses, such as order fulfillment, fraud prevention, network management, and some forms of first-party marketing, consent should be inferred. Striking the right balance in categorizing data as sensitive or non-sensitive is crucial for consumers and essential for an effective privacy law.

Requiring repetitive consumer consent for data collection and uses that are expected and raise little risk of substantial harm will not only impose unnecessary burdens on consumers, as well as businesses, it will also reduce consumers' focus on the affirmative consent requests for the types of sensitive data whose misuse may lead to more serious consequences. Second, legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. Put simply, data, and increasingly commerce, knows no State boundaries. For this reason, State intervention in this quintessentially interstate issue is problematic no matter how well-intentioned.

A proliferation of different State privacy requirements would create inconsistent protections for consumers, as well as significant compliance and operational challenges for businesses of all sizes. Federal legislation should also be technology neutral and apply to all entities across the Internet ecosystem that make use of consumer data, whether technology companies, broadband providers, or retailers, all of whom are represented on today's panel.

Third, a strong privacy law needs to include strong enforcement to protect consumers? rights. A single Federal privacy law that gives consumers more control over their data and the FTC more enforcement authority, will dramatically strengthen consumer protections. It should authorize the FTC to fine companies for first-time violations, and in certain cases, to issue rules to fill in gaps in the law and to keep up with developments in technology. It should also give the FTC more resources. State AGs should be given the power to enforce any new Federal law.

A consumer privacy law though should not include private rights-of-action that would primarily benefit lawyers and result in class actions that provide little, if any, relief to actual victims. Giving the FTC enhanced authority to provide consumer redress would be a more effective way to enable consumers to be compensated di-

rectly and promptly when companies engage in harmful data practices.

So thank you again for the opportunity to testify today and the Coalition looks forward to working with the Committee and all stakeholders to craft strong, national privacy legislation. And we applaud you for releasing drafts that will provide the foundation for Congressional action.

[The prepared statement of Ms. Ohlhausen follows:]

PREPARED STATEMENT OF MAUREEN K. OHLHAUSEN, CO-CHAIR, 21ST CENTURY PRIVACY COALITION

Chairman Wicker, Ranking Member Cantwell, and other distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing examining legislative proposals to protect consumer data privacy. My name is Maureen Ohlhausen, and I am a partner at the law firm Baker Botts L.L.P. Along with Jon Leibowitz, I also serve as co-chair of the 21st Century Privacy Coalition (Coalition).[1] I had the pleasure of serving as a Commissioner (2012–2018) and Acting Chairman (2017–2018) of our Nation's leading consumer privacy protection agency, the Federal Trade Commission (FTC).

The FTC has brought hundreds of privacy-and data security-related enforcement actions, covering both on-and offline practices and fast-evolving technologies.[2] It has creatively used every enforcement, policy, and educational tool at its disposal in its privacy and data security work to protect consumers' personal information while still allowing consumers to enjoy the benefits of the many innovative products offered in today's dynamic marketplace.

However, as the collection, use, and sharing of personal data have continued to grow in amount and complexity, and consumers and businesses are increasingly required to navigate a tangled web of confusing, and often inconsistent, data privacy regulations from various levels of government, the Coalition believes it is imperative that Congress enact comprehensive Federal privacy legislation. We therefore commend the Members of this Committee for your leadership in releasing proposed Federal privacy legislation to give stronger protections to consumers, impart clearer guidance to businesses coupled with more accountability, and provide more authority to the FTC to police harmful data practices. To avoid a patchwork of inconsistent, even conflicting, privacy requirements, Congress needs to act quickly, and the Leadership and Members of this Committee today take a very important step in that direction.

The Coalition is part of a strong consensus among businesses, civil society groups, and consumers in support of Federal privacy legislation. As an extensive survey by the Progressive Policy Institute conclusively found, consumers (1) overwhelmingly (*i.e.,* 94 percent) want the same privacy protections to apply to their personal information *regardless* of the entity that collects such information and (2) overwhelmingly (83 percent) expect to enjoy heightened privacy protections for sensitive information and for uses of their sensitive information that present heightened risk of consumer harm, again *regardless* of the company charged with maintaining it.[3]

What we all have in common is a desire for there to be clear consumer privacy protections that apply throughout the nation, no matter where you live, work, or

---

[1] The 21st Century Privacy Coalition is comprised of the Nation's leading communications providers and their trade associations, including AT&T, CenturyLink, Comcast, Cox Communications, CTIA, NCTA—The Internet and Television Association, T-Mobile, USTelecom, and Verizon.

[2] *See, e.g.,* FTC 2018 Privacy and Data Security Update, *https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.*

[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 percent of consumers favor such a consistent and technology-neutral privacy regime, and that 83 percent of consumers say their online privacy should be protected based on the sensitivity of their online data, rather than by the type of Internet company that uses their data). *See also https://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rulesprotecting-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.").

travel. We want consumers to enjoy confidence that their personal information is not subject to different protections within a state or from state to state. We are supporters of strong consumer privacy rights and believe firmly in providing transparency and control to consumers, robust security, and strong accountability as outlined in the FTC's bipartisan 2012 landmark Privacy Report.[4]

Key Elements of an Effective Federal Framework

We strongly believe that Congress needs to enact Federal privacy legislation that includes three key attributes. First, it should provide consumers clarity and visibility into companies' data collection, use, and sharing practices, as well as choices regarding these practices, calibrated to the sensitivity of that data. Second, legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. Third, it should ensure strong enforcement that protects consumer from harmful data practices, while also allowing companies to provide and develop innovative products and services that consumers want.

1. Reflect consumer preferences through simple choices based on the sensitivity of data

KWe believe that an optimal approach would balance ease of use and transparency by giving consumers clear and simple privacy choices based on the nature of the relevant information itself—its sensitivity and the risk of consumer harm if such information is the subject of an unauthorized disclosure. A Federal privacy law should promote consumer control and choice by imposing requirements for obtaining meaningful consent based on the risks associated with different kinds and uses of consumer data. We also believe that consumers should have certain rights of access, correction, and deletion where appropriate.

So-called sensitive personal information, such as health and financial information, real-time geo-location information, social security numbers, and children's information, should be subject to the highest protections. In turn, to reflect consumer expectations and preferences, there should be less-stringent requirements on *non*-sensitive personal information, as well as information that is de-identified or aggregated because such information has a lower risk of consumer harm or association with a particular individual. And, for certain types of routine operational uses, consent should be inferred. As recognized by the FTC in its 2012 Report, these uses, which include order fulfillment, fraud prevention, network management, and some forms of first-party marketing, are expected by consumers and provide them a variety of benefits, including knowing about promotions and discounts tailored to their existing services and products.

Striking the right balance in categorizing data as sensitive or non-sensitive is crucial for consumers and essential for an effective privacy law. A regime that requires consumers to constantly provide consent for data collection and uses that are expected and raise little risk of substantial harm will not only impose unnecessary burdens on consumers (as well as businesses), but will also reduce consumers' focus on the affirmative consent requests for the types of sensitive data whose misuse may lead to more serious consequences.

A Federal privacy law must also recognize that consumers have a wide variety of preferences about the benefits of sharing their personal data. Legislation should not limit consumer choice by, for example, inhibiting consumer-friendly incentive programs tied to privacy choices, such as rewards or loyalty programs. Rather, the law should require that companies give consumers clear and comprehensible information about the categories of data that are being collected, used, or shared, and the types of third parties with which information may be shared. So long as consumers are provided with clear information about the nature of such programs, they should be allowed to make their own choices, especially because such programs often involve significant cost savings and other benefits to consumers.

2. Provide a national and uniform set of protections and consumer rights throughout our digital economy

As discussed above, a new Federal privacy law should provide meaningful consumer control and choice over consumers' personal data based on the sensitivity of such information. Such 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 lines. Put simply, data (and, increasingly, commerce) knows no state boundaries. For this

[4] *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-protectingconsumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.*

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, as well as significant compliance and operational challenges for businesses of all sizes. It also erects barriers to the kind of innovation and investment that is a lifeblood of our Nation's economy and to many beneficial and consumer-friendly uses of information. Indeed, even the authors of California's 2018 privacy law recognized the wisdom of preempting municipal privacy laws.

Federal legislation should also be technology-neutral and apply to all entities across the Internet ecosystem that make use of consumer data, whether technology companies, broadband providers, or retailers, all of whom are represented on today's panel. What matters is not who collects the data, but what data is collected, how sensitive it is, and how it is protected and used.

3. Ensure strong accountability and enforcement that best protects consumer interests

The Members of this Committee recognize that Congress must develop a law that guarantees strong privacy rights to consumers and adopts best practices from state laws, while creating uniformity across the Nation. But preempting state laws should not mean weakening protections for consumers. A Federal consumer privacy law needs to be a strong one. The Coalition believes that states, as well as the FTC, have a critical role to play in protecting and enforcing those rights.

The FTC should have the primary authority to enforce a national privacy law. As privacy concerns become weightier and more complex, the FTC is reaching the limits of its current tools. Under its existing legal regime, in which the FTC polices privacy under its Section 5 authority to prevent unfair and deceptive acts or practices, when the FTC goes after a company for an initial privacy violation, it can require the company to change its practices through a consent order. In very limited circumstances, the FTC can obtain (non-punitive) monetary redress for consumers if the agency can show direct consumer losses. Only if a company later violates that order—and a judge agrees there has been such a violation—can the FTC impose a financial penalty (as opposed to obtaining consumer redress).

We believe the FTC needs to be able to fine companies for first-time violations of the new, comprehensive privacy law to provide sufficient incentives for companies to take the necessary steps to ensure responsible use and protection of consumer data. In certain cases, Congress should also give the Commission the authority to issue rules to fill in gaps in the law and to keep up with developments in technology. These rules will add clarity to the law so that companies understand what kind of behavior is out of bounds as technology and business practices evolve.

Congress must also provide the FTC with more resources to protect consumer privacy in America. Despite the ever-growing need for privacy enforcement, the FTC's budget has been flat since 2013. The number of full-time employees lags behind where it was in the early 1980s—nearly four decades ago, when the phrase "big data" meant an encyclopedia and the United States had one hundred million fewer people. The Internet and the collection, use, and sharing of consumer data have grown enormously without a similar boost in FTC resources. We urge Congress to address that widening gap if we are serious about tackling an issue as important and complicated as consumer privacy.

We also recognize that state attorneys general (AGs) are critical allies in the realm of consumer protection. They should be given the power to enforce any new Federal law. A consumer privacy law, though, should not include private rights of action, which often result in class actions that primarily benefit attorneys while providing little, if any, relief to actual victims. Private rights of action also frequently result in the diversion of company resources from compliance to litigation, which ultimately does not help consumers who, at the end of the day, simply want companies to follow the law. Nor would it be appropriate to ban pre-dispute arbitration clauses in the context of a new privacy law.

Providing the FTC and state AGs with enforcement power, backed up with civil fining authority and expanded resources, represents a far better approach for consumers, as evidenced by the successful and bipartisan work in policing violations of children's privacy through the Children's Online Privacy Protection Act. Providing the FTC with enhanced authority to provide consumer redress would also ensure that consumers can be compensated directly and promptly when companies engage in harmful data practices.

Conclusion

Thank you again for the opportunity to testify today. The Coalition looks forward to working with all Members of the Committee and all stakeholders in crafting strong national privacy legislation, and we applaud the Committee's Leadership and

other Members for releasing drafts that will provide the foundation for Congressional action.

The United States would benefit significantly from a strong and unified, technology-and industry-neutral Federal privacy law that applies uniformly to all entities, regardless of their business model. A new Federal law that preempts state laws would provide both consumers and businesses with necessary guidance and give consumers much-needed control over their data. Such a Federal law would provide the greatest clarity and certainty about the rights of consumers, as well as the responsibilities of companies that collect, use, or share consumers' personal information.

That is why a new law, backed up by an experienced and expert agency like the FTC—one with expanded powers and resources—is the best hope for consumers when it comes to meaningful privacy protections.

The CHAIRMAN. Thank you very much. Ms. Moy.

STATEMENT OF LAURA MOY, ASSOCIATE PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER; DIRECTOR, COMMUNICATIONS & TECHNOLOGY LAW CLINIC; AND ASSOCIATE DIRECTOR, CENTER ON PRIVACY & TECHNOLOGY

Ms. MOY. Thank you. Good morning, Chairman Wicker, Ranking Member Cantwell, distinguished members of the Committee. It is an honor to present before this Committee today and among such distinguished panelists, so thank you very much. Americans are desperate for greater privacy protections.

As Ms. Brill mentioned just a moment ago, 81 percent of Americans feel that the potential risks of companies collecting data about them outweigh the benefits. Almost 70 percent are not confident that companies will use their personal information in ways that they will be comfortable with. And almost 80 percent believe that if companies misuse or compromise personal information, they won't admit mistakes and take responsibility. And they are clear that they want the Government to step in. Seventy-five percent say there should be more regulation. In fact one recent poll showed that the majority of Americans feel that the threat to personal privacy online is a crisis and we need forced changes to the way companies operate.

That sounds like a directive not just to legislate but to legislate boldly in a way that transforms data practices and now is not the time for a light touch approach. And that is why I am pleased to see that there are multiple bills before this committee that offers strong, meaningful reform. That said, there certainly are differences among the bills, and I discussed many of them in my written statement but right now I would like to highlight three key things that I hope this Committee will not lose sight of as it negotiates a path forward.

First, Congress must reject privacy legislation that does not include civil rights protections. This is not just me saying this. This Committee received a letter back in February this year signed by dozens of public interest organizations, including civil rights and racial justice giants such as Asian Americans Advancing Justice, Color of Change Human Rights Campaign, Lawyers Committee, NAACP, National Organization for Women Foundation, National Urban League, The Leadership Conference, Unidos U.S., the list goes on and on.

A total of 43 organizations signed the letter urging the Committee, "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. Online discrimination is not just theoretical. Studies have shown that data-driven advertising has resulted in extreme bias in ads for housing, employment, and credit.

For example, research published this year showed that even when advertisers did not specify a demographic audience for their ads, Facebook's data driven advertising engine displayed ads for jobs in the lumber industry to an audience that was 72 percent men or 72 percent white and 90 percent men. Supermarket cashier positions were shown to 85 percent women. Jobs with taxi companies were shown to 75 percent black users. These aren't idle concerns, this is serious.

In terms of where a lack of privacy could take us, this is the worst case scenario, a future where our decisions aren't our own, where opportunities aren't available to everyone because we have been so tracked and profiled and targeted that we see a different Internet with different opportunities than other people. Many people say that America is a land of opportunity and is it? If we want to honor the American value of opportunity, we have to fight to preserve it. And I am very pleased that multiple bills before this committee would help to do that by addressing discriminatory uses of data, with the strongest provisions in the Consumer Online Privacy Rights Act bill that was introduced last week by Ranking Member Cantwell with Senators Schatz, Klobuchar, and Markey. Second, we need robust enforcement. It is not enough to create rights in name only.

We need bold action to design a law to be vigorously enforced so that data practices will change dramatically as they must. The FTC has 40 people working on privacy and data security. That is fewer people than are in this room right now. That is plainly not enough. In contrast, the UK has more than 500 people working in its information commissioner's office. Ireland's data protection commission has about 110 employees.

Adding State Attorneys General is helpful, but that too will only go so far. For example, earlier this year the Office of the California State AG said that it would have the ability to prosecute only three cases a year. It is news to no one that the country is big and if we really want the law to be enforced, we are going to need even more. The true force multiplier would be to establish a private right of action, a step that again multiple proposals before this Committee would take.

Third, Congress should not encroach on State's regulatory efforts. As Congress considers establishing new privacy and data security protections for private information, it shouldn't eliminate existing protections that already benefit Americans at the State level nor should it preempt the States' right to develop new ways to protect their citizens.

States are innovating in this space right now and making valuable contributions. I appreciate the Committee's commitment to doing something about privacy. Attempting to review the bills before the Committee and preparation for this hearing was no easy

task, as we were discussing before the hearing, because there are many of them with a variety of really interesting and great ideas.

Thank you again and I look forward to your questions.

[The prepared statement of Ms. Moy follows:]

PREPARED STATEMENT OF LAURA MOY, ASSOCIATE PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER; DIRECTOR, COMMUNICATIONS & TECHNOLOGY LAW CLINIC; AND ASSOCIATE DIRECTOR, CENTER ON PRIVACY & TECHNOLOGY

Introduction and Summary

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for inviting me here today. I am Laura Moy, an associate professor at Georgetown Law and director of the law school's Communications & Technology Law Clinic. I appreciate the opportunity to testify today on consumer privacy. I make six points:

1. *Congress must accept that a strong consumer privacy law will force business practices to change.* That change will be costly for companies. Companies may protest a strong privacy law, but Congress should take its lead from people, not companies. Congress should accept that meaningful regulation requires an adjustment period.
2. *Privacy legislation must contain use restrictions.* It is not enough to require companies merely to disclose what they plan to do with consumer data; rather, they should be restricted to uses that are reasonable. And some applications of consumer data should simply be off-limits.
3. *Congress must not accept legislation without civil rights protections.* The most troubling use of data is to facilitate discrimination. Congress should prohibit uses of data that selectively deny access to—or awareness of—opportunities in housing, education, finance, employment, and healthcare.
4. *Congress should not step on states' toes.* As Congress considers establishing new privacy and data security protections for Americans' private information, it should *not* eliminate existing protections that already benefit Americans at the state level. Nor should it preempt the states' right to develop new ways to protect their citizens. States are innovating in this space right now and making valuable contributions.
5. *There are valuable provisions in multiple bills before this committee.* The Committee should be commended for working diligently and creatively to develop legislation that meets growing demands for privacy protection.
6. *If Congress cannot agree on legislation that embodies the Public Interest Privacy Legislation Principles, it should not act.* One option before Congress is to hold its pen. If Congress cannot produce a bipartisan bill that synthesizes the valuable provisions across bills to embody the principles advanced by public interest organizations over a year ago, perhaps it should wait—and allow states to continue to fill the gap.

1. We need regulation that changes the industry

As Congress considers how best to address calls for consumer privacy protections, it should not shy away from major reforms. Congress must accept that a strong consumer privacy law will force business practices to change, and that will be costly for companies. But major change is necessary, both to address consumers' long-standing unanswered privacy concerns and to rein in harmful misuses of consumer data that should never have been allowed to become entrenched.

According to a recent poll, a majority of Americans now feel that "the threat to personal privacy online is a crisis, and we need forced changes to the way companies operate."[1] Americans overwhelmingly feel they have no control and little understanding about how their information is used. Following a large survey of thousands of U.S. adults, Pew Research Center reported in November that 81 percent say they have very little or no control over the data companies collect and 59 percent have very little or no understanding about what companies do with the data collected.[2]

---

[1] Laura Wronski, *Axios/SurveyMonkey Poll: Privacy Deep Dive,* Mar. 9, 2019, *https://www.surveymonkey.com/curiosity/surveymonkey-axios-poll-privacy-deep-dive/*.

[2] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information,* Nov. 15, 2019, *https://www.pewresearch.org/internet/*

At the same time, Americans plainly have deep privacy concerns, with the survey revealing that:

- 81 percent feel the potential risks of companies collecting data about them outweigh the benefits;
- 72 percent say they personally benefit very little or none from companies collecting data about them; and
- 79 percent are very or somewhat concerned about how companies use the data collected.[3]

These privacy concerns are distributed across industries. A whopping 85 percent of Americans are concerned a lot or a little about how much personal information social media sites know about them, 84 percent about advertisers, and 80 percent about companies they buy things from.[4]

Americans also have a striking lack of trust in companies' ability and incentives to address this problem:

- 69 percent are not too confident or not at all confident that firms will use their personal information in ways they will be comfortable with;
- 79 percent are not too confident or not at all confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information; and
- 57 percent are not too confident or not at all confident that companies follow what their privacy policies say they do with users' personal data.[5]

And Americans agree that government needs to do more to address this problem. According to the same Pew survey, 75 percent of U.S. adults say there should be more regulation than there is now. That includes both Republicans (70 percent) and Democrats (81 percent).[6]

In the absence of robust regulation, although providers of online sites and services often engage in ongoing conversations with civil rights, civil liberties, and public interest groups, they nevertheless have repeatedly failed to respect and protect data relating to millions—and at times billions—of users. In recent years the lack of strong privacy protections has led to countless highly publicized failures such as when Cambridge Analytica successfully used Facebook's platform to learn private information about many more than 87 million users, and when Google revealed that it was still tracking users' location through use of its services even after users had disabled the "Location History" feature.[7]

2. Privacy legislation must contain use restrictions

Many of our privacy laws in past years have been based on a notice and consent (or "transparency and control") framework—the idea that companies should be able to do what they please with consumer data so long as they are open about it and get permission. But it is time to recognize we need more, and to adopt meaningful use restrictions. Some uses of data are clearly harmful. In addition, consumers can no longer easily understand what they are disclosing when they share information online. The consent model also has reached the limits of scalability and is no longer feasible as a practical matter.

Consumers and policymakers alike now recognize a wide range of harms from certain data-driven content distribution models. On many platforms and services, consumer data is used to predict what advertisements, products, or other content a consumer will like or otherwise engage with so that they can be shown that information, for the purpose of maintaining their interest and generally holding them on the service for as long as possible. There are obvious incentives for companies to employ this model, under theories that (1) it is more efficient to show a consumer something she is interested in rather than waste computing power showing her something irrelevant to her, and (2) it is beneficial to keep a consumer's interest for as long as possible for the purpose of displaying more ads, products, or other content to her. But many consumers object to data-driven personalization. According to a 2019 privacy and security survey conducted by security company RSA:

2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

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

- Only 31 percent of U.S. respondents believe that tailored newsfeeds are ethical;
- Only 37 percent believe that it's ethical to make recommendations to a user based on purchase/browsing history; and
- Only 38 percent believe that using a "like" history to recommend content is ethical.[8]

Consumers are concerned about data-driven distribution models with good reason. There is growing information that these models can lead to a number of harms not only to individual consumers, but to society more broadly. For example, these models can lead to:

- Widening political polarization. Data-driven models may be more likely to promote hyper-partisan content, which in turn may exacerbate political polarization. As one prominent legal scholar has written, "Self-insulation and personalization are solutions to some genuine problems, but they also spread falsehoods, and promote polarization and fragmentation."[9]
- Dissemination of propaganda, misinformation, and disinformation. Consumer data may be used to generate and target false information, including state-sponsored propaganda, careless or low-quality reporting, and false information designed to undermine democracy.[10]
- Amplification of hate speech. Consumer data may also be used to make the distribution of hateful and racist rhetoric and calls to violence more efficient.[11]
- Public health threats. Data-driven models that equate user "engagement" with success may be designed to be addictive and inescapable.[12] Addiction to social media and other services can lead to a cascade of other problems, including heightened rates of depression, suicide, and sleep deprivation among young people.[13]
- Distribution of discriminatory advertisements. Data-driven ad distribution can result in information about critical opportunities being systematically withheld from entire classes of people.[14]

---

[8] RSA, *RSA Data Privacy & Security Survey 2019: The Growing Data Disconnect Between Consumers and Businesses* (2019), *https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf.*

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

[10] David McCabe, *Facebook Finds New Coordinated Political Disinformation Campaign,* Axios, July 31, 2018, *https://www.axios.com/facebook-finds-misinformation-campaign-4c5910b3-021a-45b7-b75c-b1ac80cbce49.html;* Dipayan Ghosh & Ben Scott, *Disinformation Is Becoming Unstoppable,* Time, Jan. 24, 2018; April Glaser & Will Oremus, *The Shape of Mis- and Disinformation,* Slate, July 26, 2018, *https://slate.com/technology/2018/07/claire-wardle-speaks-to-if-then-about-how-disinformation-spreads-on-social-media.html;* Alice Marwick & Rebecca Lewis, *Media Manipulation and Disinformation Online* (2017), *https://datasociety.net/pubs/oh/DataAnd Society_MediaManipulationAndDisinformationOnline.pdf.*

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

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

[13] Recent studies have linked the use of platforms like Facebook, Snapchat, and Instagram to depressive symptoms in young adults caused by negatively comparing oneself to others on social media platforms. Brian A. Feinstein, *et al., Negative Social Comparison on Facebook and Depressive Symptoms: Rumination as a Mechanism,* 2 Psych. Pop. Media Culture 161 (2013). *http://psycnet.apa.org/record/2013-25137-002.* Experts have also found that teens who spend three hours a day or more on electronic devices are 35 percent more likely to have a risk factor for suicide and 28 percent more likely to get less than seven hours of sleep. Jean M. Twenge, *Have Smartphones Destroyed a Generation?,* The Atlantic, Sept. 2017, *https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198/.* Data-driven content distribution has also led to the proliferation of dangerous health-related misinformation. *See, e.g.,* Christine Hauser, *Drinking Bleach Won't Cure Autism or Cancer, F.D.A. Says,* N.Y. Times, Aug. 13, 2019, *https://www.nytimes.com/2019/08/13/health/drinking-bleach-autism-cancer.html* (the FDA was forced to counter medical misinformation telling consumers to drink bleach solutions as cures for autism, cancer, H.I.V./AIDS, and other conditions).

[14] *See generally* Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, & Aaron Rieke, *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes,* Proceedings of the ACM on Human-Computer Interaction (2019), *https://arxiv.org/abs/1904.02095* [hereinafter *Discrimination Through Optimization*].

Use restrictions may not be able to prevent all of these harms entirely, but should prohibit at least the most egregious misuses of data, as well as create obligations for companies that employ data-driven distribution models to detect problems such as those described here and take steps to address them.

Use restrictions are also needed because meaningful consent is no longer feasible in all circumstances as a practical matter.[15] There are too many data exchanges every single day for consumers realistically to understand all of them and read every privacy policy.[16] And as we become surrounded by always-on connected devices, it is increasingly difficult for companies to solicit and receive consent. It remains important for companies to be transparent about their practices and to be required to observe user rights attaching to consumer data, but use restrictions would provide a much-needed backstop to protect against inappropriate uses of data.

In addition, use restrictions are needed because it has become exceptionally difficult for consumers to understand what they are disclosing when they share information online. Today, very sensitive information about a consumer can be inferred from data that seems less sensitive. For example:

- Cell phone sensors might be used to infer whether or not someone has Parkinson's;[17]
- Data about brushing habits collected by a person's toothbrush app might be used to infer health status, travel patterns, and relationship status;[18] and
- Location data might be used to infer where a person works, lives, and worships, where their kids go to school, and the facility where they seek medical treatment.[19]

This Committee should seek to further develop use restrictions in privacy legislation. Two bills before the Committee contain provisions that serve as good starting points. The Consumer Online Privacy Rights Act (COPRA) introduced just last week by Ranking Member Cantwell and Senators Schatz, Klobuchar, and Markey, as well as the Privacy Bill of Rights Act introduced by Senator Markey, prohibit discriminatory uses of data as described above, as well as certain uses of biometric information.[20]

Notice and consent has clear limits. For privacy legislation to protect consumers, it must contain meaningful use limitations as well.

3. Congress must not accept legislation that does not contain civil rights protections

Congress should reject out of hand any consumer privacy proposal that does not contain civil rights protections. If Congress is going to legislate, it should legislate for all consumers. One important way to do this is to ensure that consumer data cannot be used to facilitate discrimination or otherwise to selectively deny access

---

[15] There is a lengthy discussion of this problem in the testimony of Professor Woodrow Hartzog before this Committee earlier this year. *See* Prepared Testimony and Statement for the Record of Woodrow Hartzog before the Senate Committee on Commerce, Science, and Transportation regarding "Policy Principles for a Federal Data Privacy Framework in the United States (Feb. 27, 2019), available at *https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53.*

[16] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S:J. L. & Pol'y for Info. Soc'y 1, 9 (2008), *http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf* (estimating the national opportunity cost for the time it would take Americans to read every privacy policy they come across at $781 billion); Joel R. Reidenberg, N. Cameron Russell, Alexander J. Callen, Sophia Qasir, & Thomas B. Norton, *Privacy Harms and the Effectiveness of the Notice and Choice Framework,* 11 I/S: A Journal of Law and Policy 485, 492 (2014) ("To start, there are simply too many privacy policies to keep track of, given the potentially hundreds of websites a user might visit on any given day. To read all of these privacy policies would be extremely time consuming and extremely costly.").

[17] Ana de Barros, *Parkinson's DREAM Challenge Uses Mobile Sensor Data to Monitor Health Based on Movement,* Parkinson's News Today, July 20, 2017, *https://parkinsonsnewstoday.com/2017/07/20/parkinsons-digital-dream-challenge-uses-smartphones-remote-sensing-data-monitor-health/.*

[18] *See* Justin Peters, *Should This Thing Be Smart? Toothbrush Edition.,* Slate, Mar. 12, 2018, *https://slate.com/technology/2018/03/should-this-thing-be-smart-colgate-connect-e1-smart-toothbrush-edition.html.*

[19] *See* Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret,* N.Y. Times, Dec. 10, 2018, *https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.*

[20] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019) (as introduced by S. Cantwell to the S. Comm. on Commerce, Sci., and Transp.); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).

to—or awareness of—critical opportunities in housing, education, finance, employment, and healthcare.

Indeed, the public interest community has been consistent in its insistence that antidiscrimination must be a part of any consumer privacy law. The Public Interest Privacy Legislation Principles signed by 34 organizations in November 2018 state, "Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws."[21] In February, 47 organizations sent a letter to this Committee that stated in part,

> 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. Online services should not be permitted to use consumer data to discriminate against protected classes or deny them opportunities in commerce, housing, employment, or full participation in our democracy. Congress should require companies to be transparent about their collection and use of personal information in automated decision-making. Companies must also anticipate and protect against discriminatory uses and disparate impacts of data.[22]

In April, many of those organizations sent this Committee a follow-up letter reiterating the importance of centering civil rights concerns and urging Congress to:

1) Prohibit the use of personal data to discriminate in employment, housing, credit, education, or insurance—either directly or by disparate impact.
2) Prohibit the use of personal data to discriminate in public accommodations and extend such protections to businesses that offer goods or services online.
3) Prohibit the use of personal data to engage in deceptive voter suppression.
4) Require companies to audit their data processing practices for bias and privacy risks.
5) Require robust transparency at two tiers: easy-to-understand privacy notices for consumers, and comprehensive annual privacy reports for researchers and regulators. Companies must completely disclose how they collect and use personal data, including their algorithmic processing practices.
6) Enable researchers to independently test and audit platforms for discrimination.
7) Empower a Federal agency with rulemaking authority, enforcement powers, and enough resources to address current and future discriminatory practices.
8) Provide individual rights to access, correct, and delete one's personal data and inferences made using that data.
9) Provide a private right of action. Marginalized communities historically have not been able to rely upon the government to protect their interests, so individuals need to be able to vindicate their own rights.
10) Establish baseline nationwide protections and allow states to enact stricter laws. Under no circumstances should Congress enact any legislation that could preempt state civil rights laws, many of which are stronger than Federal law. For example, many states extend greater antidiscrimination protections to the LGBTQ+ community than Federal law.[23]

Congress must honor these requests from the public interest community because at present, these impermissible uses of information are widespread. For example, Facebook made assurances in 2017 to tackle discriminatory advertising on its platform after facing public outrage and pressure from advocates regarding its "ethnic affinity" advertising clusters, but the Washington State Attorney General later found that it was still possible to exclude people from seeing advertisements based

---

[21] *Public Interest Privacy Legislation Principles,* Nov. 2018, *https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf.*

[22] The Leadership Conference on Civil & Human Rights, *Over 40 Civil Rights, Civil Liberties, and Consumer Groups Call on Congress to Address Data-Driven Discrimination,* Feb. 13, 2019, *https://civilrights.org/2019/02/13/over-40-civil-rights-civil-liberties-and-consumer-groups-call-on-congress-to-address-data-driven-discrimination/.*

[23] Letter from 26 civil society organizations to House and Senate Commerce Committees calling for prioritization of civil rights considerations in privacy legislation, Apr. 19, 2019, *https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf.*

on protected class membership.[24] Earlier this year civil rights organizations settled lawsuits with Facebook over charges that the platform enabled landlords and real estate brokers to exclude families with children, women, and other protected classes of people from receiving housing ads, and also facilitated gender discrimination in job ads.[25]

The systematic targeting and exclusion of communities can be a byproduct of algorithmic content and ad distribution that optimizes for cost-effectiveness and user "engagement," which can lead to distribution that is discriminatory in impact, if not intent.[26] For example, this year a team of researchers found that when sponsored employment ads were posted on Facebook for a wide range of positions, including janitors, nurses, lawyers, the platform's algorithms delivered ads in a way that demonstrated clear race and gender bias.[27] More specifically, the platform displayed ads for jobs in the lumber industry to an audience that was 72 percent white and 90 percent men, for supermarket cashier positions to 85 percent women, and for jobs with taxi companies to 75 percent black users. This type of discriminatory outcome occurred even though the advertisers never specified a demographic audience for the ads.

To prevent these types of unacceptable outcomes, any new privacy legislation should outright prohibit the use of consumer data to facilitate discrimination, and also should force companies to conduct their own forecasting and testing to determine whether discrimination is occurring on their platform or is likely to occur.

Multiple bills attempt to deliver in this area. COPRA is the only bill before this committee that would both prohibit discriminatory uses of data and force companies to take steps to determine whether their data practices are likely to lead to discriminatory outcomes.[28] Others that would prohibit discriminatory uses of data include the Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act) introduced by Senator Cortez Masto and the Privacy Bill of Rights Act.[29] The Algorithmic Accountability Act of 2019 introduced by Senators Wyden and Booker would also force prospective impact assessments.[30] Congress should look to provisions in these bills for guidance on this matter.

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

4. Congress should not encroach on states' innovative regulation

As Congress considers establishing new privacy and data security protections for Americans' private information, it should not step on the toes of states also racing to protect their citizens in the face of rising privacy threats. Americans are asking for *more* protections for their private information, not less. States are responding to that call.

Indeed, a number of state laws play an important role in filling gaps that exist in Federal legislation. Many states have expanded the scope of their data security and breach notification laws to extend protections to previously unregulated market sectors and private data—and consumers in those states are benefiting from those existing laws. For example, Connecticut's data security and breach notification stat-

---

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

[25] Communications Workers of America, *Facebook Agrees to Sweeping Reforms to Curb Discriminatory Ad Targeting Practices* (Mar. 19, 2019), *https://cwa-union.org/news/releases/facebook-agrees-sweeping-reforms-curb-discriminatory-ad-targeting-practices.*

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

[27] Ali, *et al., Discrimination Through Optimization, supra* note 14.

[28] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[29] Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act), S. 583, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019).

[30] 116th Cong. (2019); Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Cong. (2019).

ute covers entities operating at multiple nodes of the health care pipeline.[31] California adopted a data security statute—the Student Online Personal Information Protection Act (SOPIPA)—that is tailored to online educational platforms.[32] SOPIPA prompted twenty-one other states to adopt student data security laws modeled on California's example.[33] Minnesota adopted a law requiring Internet Service Providers (ISPs) to maintain the security and privacy of consumers' private information.[34] And Texas now requires any nonprofit athletic or sports association to protect sensitive personal information.[35]

Some states have also expanded the types of information that data holders are responsible for protecting from unauthorized access, or for notifying consumers of when breached. For example, ten states have expanded breach notification laws so that companies are now required to notify consumers of unauthorized access to their biometric data—unique measurements of a person's body that can be used to determine a person's identity.[36] This important step recognizes that a biometric identifier such as a fingerprint or iris scan—unlike an alphanumeric password—cannot be changed after it has been compromised. A large number of states also now require companies to notify consumers about breaches of medical or health data—information that can be used in aid of medical identity theft, potentially resulting in fraudulent healthcare charges and even introduction of false information into one's medical record.[37]

And states are doing other important work on privacy as well. In addition to the California Consumer Privacy Act,[38] California also has a law requiring notification about breaches of information collected through an automated license plate recognition system.[39] Vermont has the Data Broker Act.[40] Illinois has the Biometric Information Protection Act.[41] Earlier this year, Maine enacted a new broadband privacy law.[42]

To avoid doing harm to consumers benefiting from these existing consumer protections, any Federal legislation on privacy or data security must preserve strong state standards, as well as states' ability to continue innovating on privacy. There are bills currently before the Committee that can be used as a model for crafting this provision. A number of privacy bills before this Committee are silent on preemption of state laws and presumably would only invalidate those that are in conflict. Bills that would expressly avoid preemption of stronger state laws include the Algorithmic Accountability Act and COPRA.[43] In contrast, bills that would explicitly preempt state laws—even those that offer consumers stronger privacy protections and potentially even general consumer protection laws—include the Balancing the

---

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

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

[33] Rachel Anderson, *Last Year's Education Data Privacy Legislation* Trends, iKeepSafe Blog, Jan. 17, 2018, *https://ikeepsafe.org/last-years-education-data-privacy-legislation-trends/*.

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

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

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

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

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

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

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

[41] 740 ILCS 14/1 *et seq.*

[42] Inside Privacy, *Maine Enacts Broadband Privacy Law,* June 28, 2019, *https://www.insideprivacy.com/united-states/state-legislatures/maine-enacts-broadband-privacy-law/*.

[43] Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Cong. (2019); Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

Rights Of Web Surfers Equally and Responsibly Act of 2019 (BROWSER Act) introduced by Senator Blackburn and the U.S. Consumer Data Privacy Act.[44]

5. There are valuable provisions in multiple bills before this committee

The public interest community has asked for a number of major reforms to set things right. Proposals before this committee contain provisions that would deliver many of those reforms, and the Committee can use those provisions as models to develop legislation that honors the Public Interest Privacy Legislation Principles.[45] For example, provisions in legislation before this Committee would establish a number of the items outlined in those Principles:

- *Consumer rights to data access, quality, portability, and security.* Bills that would give consumers important rights to data access, quality, portability, and security include COPRA and the Privacy Bill of Rights Act, as well as the U.S. Consumer Data Privacy Act discussion draft circulated last week by Senator Wicker.[46]
- *Data minimization.* The Privacy Bill of Rights Act should serve as a model on this point, because it would prohibit the collection of personal information unless it is needed to perform a contract, to provide a requested product or service, or to take steps at the request of the individual.[47] COPRA would prohibit the collection and retention of personal information not covered by the covered entity's articulated purposes as expressed in a privacy policy.[48]
- *A prohibition on discriminatory uses of data.*[49] Congress should look to COPRA as a model on this point, because it prohibits discriminatory uses of data, and also would force companies to take steps to determine whether their data practices are likely to lead to discriminatory outcomes.[50] Other bills that would prohibit discriminatory uses of data include the DATA Privacy Act and the Privacy Bill of Rights Act.[51] The Algorithmic Accountability Act also provides another example of how companies could be made to detect discriminatory outcomes resulting from their practices.[52]
- *Robust rulemaking authority for a Federal agency.* Bills that would establish robust rulemaking authority for a Federal agency include COPRA, the Privacy Bill of Rights Act, and the DATA Privacy Act, and these bills can be used as models for crafting agency rulemaking authority.[53] Some bills would only grant much more limited rulemaking authority. For example, the U.S. Consumer Data Privacy Act discussion draft would only give the FTC rulemaking authority to establish requirements for covered entities to verify requests associated with privacy rights, but not to honor those rights more broadly.[54] Other bills would grant rulemaking authority limited to a narrower scope of privacy coverage, such as the Commercial Facial Recognition Privacy Act of 2019 introduced by Senators Blunt and Schatz, the Deceptive Experiences To Online Users Reduction Act (DETOUR Act) introduced by Senators Warner and Fischer, the Algorithmic Accountability Act of 2019, the Do Not Track Act introduced by Senator Hawley, the Data Broker List Act of 2019 introduced by Senators

---

[44] Balancing the Rights of Web Surfers Equally and Responsibly Act of 2019, S. 1116, 116th Cong. (2019) (as introduced by S. Blackburn to the S. Comm. on Commerce, Sci., and Transp.); U.S. Consumer Data Privacy Act of 2019, available at *https://aboutblaw.com/NaZ* (discussion draft circulated by S. Wicker in Nov. 2019).

[45] *See* Public Interest Privacy Legislation Principles, *https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf.*

[46] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019); U.S. Consumer Data Privacy Act of 2019, available at *https://aboutblaw.com/NaZ* (discussion draft circulated by S. Wicker in Nov. 2019).

[47] Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).

[48] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[49] *See* discussion *supra* at Section 3, p. 7.

[50] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[51] Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act), S. 583, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).

[52] Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Cong. (2019).

[53] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019); Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act), S. 583, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).

[54] U.S. Consumer Data Privacy Act of 2019, available at *https://aboutblaw.com/NaZ* (discussion draft circulated by S. Wicker in Nov. 2019).

Peters and McSally, and the Protecting Privacy in Our Homes Act introduced by Senator Gardner.[55]

- *Additional staff and resources for an expert agency.* COPRA should serve as a model to grant staff and resources for an expert agency, because it would enable the Federal Trade Commission to form a new privacy and data security bureau, and authorization appropriations for the Commission to carry out all activities associated with the law.[56] The DATA Privacy Act would enable the Commission to appoint additional personnel and authorize appropriations for that purpose.[57] The U.S. Consumer Data Privacy Act would authorization appropriations to assist the Commission with enforcement, but not rulemaking or oversight.[58] The Markey-Hawley bill updating the Children's Online Privacy Protection Act would add a Youth Privacy and Marketing Division to the Federal Trade Commission.[59]
- *Enforcement rights not only at the Federal level, but also for state attorneys general and private citizens.* COPRA should serve as a model on enforcement. It would enable individuals to vindicate their own rights in court, and importantly also clearly provides guidelines for meaningful relief.[60] The Privacy Bill of Rights Act also contains language that crafts a private right of action.[61] Most privacy bills currently before this Committee also include critical enforcement powers for state attorneys general. Those that do not include the DETOUR Act, the BROWSER Act, the Data Broker List Act of 2019, and the Protecting Privacy in Our Homes Act.[62]
- *A prohibition on forced arbitration.* Congress should look to COPRA and the Privacy Bill of Rights Act for language prohibiting privacy-related forced arbitration.

A number of proposals also contain other substantial reform measures. For example, COPRA would expressly protect privacy whistleblowers from retaliation for providing information to enforcers.[63] The Do Not Track Act introduced by Senator Hawley would institute a Do Not Track system and require operators of sites and services to honor Do Not Track signals by refraining from data collection.[64] The Data Broker List Act would facilitate enrollment of data brokers in a national registry and place certain restrictions on data brokers.[65] And the Markey-Hawley children's privacy bill would strengthen privacy protections for children and minors.[66]

6. If Congress cannot agree on legislation that embodies the Public Interest Privacy Legislation Principles, perhaps it should not act

One option before Congress is to hold its pen. Although there are many valuable provisions in bills before this Committee that Congress can draw from as it continues to work toward comprehensive consumer privacy legislation, Congress has yet to produce a bipartisan bill that embodies the Public Interest Privacy Legislation Principles advanced by 34 public interest organizations over a year ago and attached here.[67] It is better for Congress to wait—and allow the states to continue

---

[55] Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019); Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. (2019); Algorithmic Accountability Act of 2019, H.R. 2231, S. 1108, 116th Cong. (2019); Do Not Track Act, S. 1578, 116th Cong. (2019); Data Broker List Act of 2019, S. 2342, 116th Cong. (2019); Protecting Privacy in Our Homes Act, S. 2532, 116th Cong. (2019).

[56] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[57] Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act), S. 583, 116th Cong. (2019).

[58] U.S. Consumer Data Privacy Act of 2019, available at *https://aboutblaw.com/NaZ* (discussion draft circulated by S. Wicker in Nov. 2019).

[59] A bill to Amend the Children's Online Privacy Protection Act of 1998 to Strengthen Protections Relating to the Online Collection, Use, and Disclosure of Personal Information of Children and Minors, and for Other Purposes, S. 748, 116th Cong. (2019).

[60] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[61] Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).

[62] Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. (2019); Balancing the Rights of Web Surfers Equally and Responsibly Act of 2019, S. 1116, 116th Cong. (2019); Data Broker List Act of 2019, S. 2342, 116th Cong. (2019); Protecting Privacy in Our Homes Act, S. 2532, 116th Cong. (2019).

[63] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[64] Do Not Track Act, S. 1578, 116th Cong. (2019).

[65] Data Broker List Act of 2019, S. 2342, 116th Cong. (2019).

[66] A bill to Amend the Children's Online Privacy Protection Act of 1998 to Strengthen Protections Relating to the Online Collection, Use, and Disclosure of Personal Information of Children and Minors, and for Other Purposes, S. 748, 116th Cong. (2019).

[67] *See* Public Interest Privacy Legislation Principles, *https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf.*

to fill the gap—than to rush to pass something that does not fulfill these important principles.

7. Conclusion

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

PUBLIC INTEREST PRIVACY LEGISLATION PRINCIPLES

Unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly. Surveys show that, while individuals often try to remove or mask their digital footprints,[1] people think they lack control over their data,[2] want government to do more to protect them,[3] and distrust social media platforms.[4]

The current U.S. data privacy regime, premised largely upon voluntary industry self-regulation, is a failure. Irresponsible data practices lead to a broad range of harms, including discrimination in employment, health care, and advertising, data breaches, and loss of individuals' control over personal information. Existing enforcement mechanisms fail to hold data processors accountable and provide little-to-no relief for privacy violations.

The public needs and deserves strong and comprehensive Federal legislation to protect their privacy and afford meaningful redress. Privacy legislation is essential to ensure basic fairness, prevent discrimination, advance equal opportunity, protect free expression, and facilitate trust between the public and companies that collect their personal data. Legislation should reflect at least the following ideas and principles:

1. Privacy protections must be strong, meaningful, and comprehensive

Privacy concerns cannot be fully addressed by protecting only certain classes of personal data held by some companies. Legislation should mandate fairness in all personal data processing, respect individuals' expectations for how data should be treated, provide for data portability, and include safeguards against misuse of data, including de-identified and aggregate data. Legislation should advance fundamental privacy rights and require all entities that collect, store, use, generate, share, or sell (collectively, "process") data both online and offline to comply with Fair Information Practices[5] (collection limitation, dataquality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability) across the complete life cycle of the data. Legislation should require all data processing to be clearly and accurately explained, justified, and authorized by the individual. People should have the right to know when their data has been compromised or otherwise breached. Additionally, legislation should require entities processing data to adopt technical and organizational measures to meet these obligations, including risk assessments of high-risk data processing.

2. Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity

Legislation should ensure fundamental fairness of and transparency regarding automated decision-making. Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws. Legislation must ensure that regulators are empowered to prevent or stop harmful action, require appropriate algorithmic accountability, and create avenues for individuals to access information necessary to prove claims of discrimination. Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the el-

---

[1] *The State of Privacy in Post-Snowden America,* Pew (Sept. 21, 2016), *http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america.*

[2] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data,* Consumer Reports (May 18, 2017), *https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data.*

[3] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns,* Pew (Mar. 27, 2018), *http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.*

[4] *Id.*

[5] Fair Information Practices are similar to those adopted by the OECD. *See* OECD Privacy Framework, *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.*

derly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices. Anti-discrimination provisions, however, must allow actors to further equal opportunity in housing, education, and employment by targeting underrepresented populations where consistent with civil rights laws. Moreover, decades of civil rights law have promoted equal opportunity in brick-and-mortar commerce; legislation must protect equal opportunity in online commerce as well.

3. Governments at all levels should play a role in protecting and enforcing privacy rights

The public consistently call for government to do more, not less, to protect them from misuse of their data. Legislation should reflect that expectation by providing for robust agency oversight, including enhanced rulemaking authority, commensurate staff and resources, and improved enforcement tools. Moreover, no single agency should be expected to police all data processors; therefore, legislation should empower state attorneys general and private citizens to pursue legal remedies, should prohibit forced arbitration, and importantly, should not preempt states or localities from passing laws that establish stronger protections that do not disadvantage marginalized communities.

4. Legislation should provide redress for privacy violations

Individuals are harmed when their private data is used or shared in unknown, unexpected, and impermissible ways. Privacy violations can lead to clear and provable financial injury, but even when they do not, they may, for example, cause emotional or reputational harm; limit awareness of and access to opportunities; increase the risk of suffering future harms; exacerbate informational disparities and lead to unfair price discrimination; or contribute to the erosion of trust and freedom of expression in society. In recognition of the many ways in which privacy violations are and can be harmful, legislation should avoid requiring a showing of a monetary loss or other tangible harm and should make clear that the invasion of privacy itself is a concrete and individualized injury. Further, it should require companies to notify users in a timely fashion of data breaches and should make whole people whose data is compromised or breached.

Signed,

Access Humboldt
Access Now
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Democracy & Technology
Center for Digital Democracy
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
Color of Change
Common Cause
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumers Union
Customer Commons
Demand Progress
Free Press Action Fund
Human Rights Watch
Lawyers' Committee for Civil Rights Under Law
Media Alliance
Media Mobilizing Project
National Association of Consumer Advocates
National Consumer Law Center
National Consumers League
National Digital Inclusion Alliance
National Hispanic Media Coalition
New America's Open Technology Institute
Oakland Privacy
Open MIC (Open Media and Information Companies Initiative)
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG
United Church of Christ, OC Inc.

The CHAIRMAN. Thank you very much. Ms. O'Connor.

STATEMENT OF NUALA O'CONNOR, SENIOR VICE PRESIDENT AND CHIEF COUNSEL, DIGITAL CITIZENSHIP, WALMART INC.

Ms. O'CONNOR. Thank you, Chairman Wicker. Thank you, Ranking Member Cantwell, members of the Committee. It is an honor to be with you today and to be a part of this distinguished panel. My name is Nuala O'Connor and I serve as the Senior Vice President and Chief Counsel for Digital Citizenship at Walmart.

Walmart is using technology and data to help our customers save money and live better. Walmart customers, the busy working families of America, have integrated technology into almost every aspect of their daily lives and we are trying to respond to their needs and how they shop. For example, connecting our app to our in-store experience helps make it easier to return items purchased online, to scan receipts, and keep track of what you have spent this holiday season, and allows our customers to seamlessly and securely understand their shopping experience.

Data, both about products and about customers, is helping us better source and manage our supply chain more efficiently and quickly ship orders and helps us anticipate our customers' needs. Walmart is using data in every way from food safety to responding to weather emergencies for our associates and customers. We at Walmart believe that data and technology can help our customers save money and live better, and Walmart also recognizes that while personal data does enhance the consumer experience, it also creates meaningful responsibility on the part of the companies that hold it.

Walmart's goal is quite simply to be the country's most trusted retailer. And just as our customers trust Walmart to provide them everyday low prices, quality goods, and a fast and friendly store experience, so too our customers trust us to protect their data and to use their data in a way that benefits them. I joined Walmart because it is already leading the way in the responsible use of data and technology in our daily lives. Walmart is living these values, including respect for the individual, as it deploys data and technology to serve the customers' needs. Respect for an individual for us means meeting people where they are, literally in the stores and online, and in all cases safeguarding their transactions and their identity.

Our business is selling products to the customer, not selling the customers' personally identifiable information. Walmart is committed to working with policymakers to create public policy that enhances consumer privacy, whether these customers exist in the physical world, the digital world, or increasingly as is the case, both. We strongly support the bipartisan efforts of the members of this Committee as we work toward a national privacy law that protects the rights of all consumers in the United States.

Toward that goal, we would like to offer the following points for the Committee's consideration. First, as has already been said, a comprehensive privacy law is urgently needed at the Federal level. A patchwork of inconsistent State laws is insufficient to protect the individual and is inefficient for interstate commerce. Second, legislation focused on a particular industry sector must be carefully crafted to avoid unintended effects on retail or other sectors.

And third, a comprehensive privacy law must consider the needs and operations of companies online, offline, and in the blended or Omni-channel model. Legislation must not disadvantage or privilege similar activities in the digital or physical world. As a longtime privacy professional, I am delighted to see momentum toward a comprehensive Federal privacy law, most recently in the drafts released last week by Chairman Wicker and Ranking Member Cantwell. We greatly appreciate the transparency and consumer

rights created in both proposals, the emphasis on data security which is so essential to maintaining personal privacy, the specific provisions that recognize commonly controlled and branded identities, and the recognition that data is used for broader consumer benefits such as product recalls.

We appreciate the balance struck by Chairman Wicker with structured rulemaking authority at the Federal Trade Commission, and we do share broader industry concerns with Ranking Member Cantwell's draft related to the provisions on private rights of action and preemption. We also believe some elements of both proposals have serious concerns for legitimate and beneficial uses of technology, such as using data to shorten wait times at our stores, communicating with customers about the timing of their grocery pickups, and otherwise facilitating the customer experience and transaction efficiency.

Thank you again, Chairman Wicker and Ranking Member Cantwell for the opportunity to share a little about how Walmart works to maintain and safeguard our customers' trust. We strongly support your efforts to update public policy to reflect the daily reality of our customers, whose retail habits include online transactions, store transactions, and many that are combination of both. We look forward to supporting your efforts as you work toward a national Federal privacy law. I stand ready to answer your questions. Thank you.

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

PREPARED STATEMENT OF NUALA O'CONNOR, SENIOR VICE PRESIDENT AND CHIEF COUNSEL FOR DIGITAL CITIZENSHIP, WALMART INC.

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to be here today. It is an honor to be part of such a distinguished panel. My name is Nuala O'Connor and I serve as the Senior Vice President and Chief Counsel for Digital Citizenship at Walmart. Walmart is a leading retailer serving customers in stores, online, and through their mobile devices. As our customers' shopping habits and expectations have changed, Walmart continues to evolve to meet their needs.

Our customers have integrated technology into almost every aspect of their daily lives—including how they shop. Our customers expect a seamless experience, in store and online.

Walmart is using technology and data to help our customers save both time and money. For example, connecting our app to our stores makes it easier to return items in a store after purchasing online. Data—both about products and about customers—is helping us better source and manage our supply chain, more efficiently and quickly ship orders, and helps us anticipate customers' needs. Walmart is also using data and technology to improve food safety and respond to weather emergencies for our associates and customers. Indeed, it is very appropriate that we are talking about service and shipping and shopping today. Did you know there are only 21 shopping days until Christmas?

We at Walmart believe that data and technology can help our customers save money and live better. Walmart also recognizes that while personal data can enhance the customer experience, it creates responsibility on the part of the companies that hold it.

Walmart's goal is, quite simply, to be the country's most trusted retailer. Just as our customers trust Walmart to provide *every day low prices,* quality goods, and a *fast and friendly* store experience, so too our customers trust us to protect their data, and to use that data in a way that benefits them. While technology may have changed how we operate our business, it has not—and it will not—change our values.

In my brief time at Walmart, I've learned the importance the company places on its core values, including *Respect for the Individual.* It means meeting people where they are with dignity. In store, it means we greet our customers and help them find

what they need. Online, it also means we greet our customers and help them find what they need. And in all cases, we safeguard their transactions and identity. Our business is selling products to the customer, *not* selling the customer's personally identifiable information.

Walmart is committed to working with policymakers to create public policy that will enhance consumer privacy, whether we meet those customers in the physical world, in the digital world, or, as is increasingly the case, both. We strongly support the *bipartisan* efforts of Members of this Committee as we work towards a national privacy law that protects the rights of all consumers in the United States.

Broadly, we support:

- *Customer Control*—Customers should have reasonable controls with regard to the collection, use and sharing of personal data. Customers should have an opportunity to reasonably access, correct or delete their data while limiting the sale of their data to third parties and its use in digital advertising.
- *Retail Sensibility*—Federal privacy policy should reflect a world blended with physical and digital experiences.
- *Consistency*—Policymakers should harmonize U.S. privacy legislation, preempting a patchwork of state laws.
- *Flexibility*—The rights and obligations of a national framework should be sufficiently flexible to preserve the ability for companies to innovate for their customers.

Towards that goal, we would like to offer a few reflections for the Committee's consideration:

First, a comprehensive Federal privacy law is urgently needed; a patchwork of inconsistent state law is insufficient to protect individual privacy and is inefficient for interstate commerce.

Because our roots are in the physical world, our perspective may differ from companies that operate primarily online. Walmart operates more than 4,700 stores in the United States. Each week, nearly 160 million people around the country shop with us—either at one of our stores or online. Our stores are present in local communities and are part of Americans' daily lives in every state. Our customers often know our store associates by name and these personal relationships build trust. When customers buy something from our shelves, they trust us to have sourced it responsibly and to have priced it accordingly. They trust it to be a genuine product. They trust that they are being treated fairly.

Responsible data privacy is part of that trust. Building that trust requires clarity and consistency. While states have an important part to play, a patchwork of state laws would only serve to complicate, not clarify, the customer experience. For example, if I use my Walmart app, which you should all download if you haven't already, on my 516-area code number, from my home in Maryland, to order the WoodWick Frasier Fir holiday candle to send to my sister in New Jersey (which in fact I did just last week—it's amazing), from our website hosted in California, and the candle is shipped from Arkansas, which state privacy law would the company need to adhere to as it processes my data? My state? Or my sister's? Alternatively, if a customer lives on the California border and shops at a Walmart in Nevada, does the Nevada store necessarily then give that customer, or all customers, California rights? Absent alignment on state privacy laws, these implementation questions add complexity, uncertainty, and cost for the customer and company alike.

Second, legislation focused on a particular industry sector must be carefully crafted to avoid unintended effects on retail or other sectors.

For example, the concept of data portability was originally intended to provide greater control over an individual's social media communications or online accounts. However, data portability may have negative consequences in a blended business model or other industries. Should a national privacy law require us to directly port our customer data to another competitor, even in aggregated form, we are concerned that this data could be reverse engineered and allow competitors to discern proprietary business information and processes. Additionally, we have concerns about the security of customer data while in transit. We believe that the concept of data portability must simultaneously recognize values of individual privacy, technological innovation, and data security. We appreciate the work of Senators Warner, Hawley, and Blumenthal on data portability in their ACCESS Act (S. 2658) and we hope to see similarly nuanced treatment of data portability in the bipartisan bill.

Third, a comprehensive privacy law must consider the needs and operations of companies online, offline, and blended, or omnichannel. Legislation focused solely on the online space must not disadvantage or privilege similar activity in the physical world.

In my time at Walmart, I've learned a lot of acronyms, and so one I want to leave with you to day is: BOPI. What is a BOPI? It is a transaction where you buy something online and pick up instore. Walmart is doing great things with online grocery ordering and instore pickup and I encourage you to check it out. I did my first BOPI a few years ago, when I was buying a new bicycle for my daughter. As a busy working mother, I was scouring the Internet late one night for deals on this particular yellow bike she wanted. Many excellent retailers could have sent it to us and dropped it, unassembled, on my front porch. But Walmart had it ready for pickup, already assembled. I walked in and showed them my phone with the purchase information, and I spent the weekend riding bikes with my children, instead of putting that bike together. That's the success of online ordering and instore pickup. It saved my family time and money, and allowed us to live better. That is our goal, and we hope legislation will provide a level playing field for companies, whether online, offline, or omnichannel—which is both.

Data portability is just one example of how policy to address digital actors can have unintended consequences for retail operations. We look forward to a continued dialogue with Members of this Committee to better understand things such as whether or not retailers are considered "edge providers" and how algorithm notification should apply to retail websites where sometimes hundreds of algorithms are used to create a seamless, consumer-requested personalization.

As a longtime privacy professional, I am delighted and grateful to see this momentum towards a comprehensive privacy law. Most recently, in the drafts released last week by Chairman Wicker and Ranking Member Cantwell, we greatly appreciate the transparency and consumer rights created by both proposals; the emphasis on data security—which is so essential to maintaining personal privacy; the specific provisions that recognize commonly controlled and branded entities; and the recognition that data is used for broader consumer benefits, such as product recalls. We appreciate the balance struck by Chairman Wicker with structured rulemaking authority for the Federal Trade Commission. Conversely, we share broader industry concerns with Ranking Member Cantwell's draft related to provisions on private rights of action and preemption. We also believe some elements of both proposals could impede legitimate and beneficial uses of technology, such as using data to shorten wait times at our stores; communicating with customers about the timing of grocery pickups; and otherwise facilitating the customer experience and transaction efficiency.

Finally, regarding data practices at Walmart, please see the attached appendix. Thank you again, Chairman Wicker and Ranking Member Cantwell, for the opportunity to share how Walmart works to maintain and safeguard our customers' trust. We strongly support your efforts to update public policy to reflect the reality of our customers, whose retail habits include online transactions, store transactions, and some that are a combination of both. We look forward to supporting your efforts as you work towards a national privacy law. I stand ready to answer any questions you may have.

APPENDIX: DATA USAGE AT WALMART

We look forward to a continued dialogue during this process as we work to ensure customers' rights are protected not just in retail but across all industries.

Below please see data practices and usage as they apply to Walmart Inc. in the U.S., which includes Walmart Stores, Sam's Club and several recently acquired companies. Our customer-facing privacy policies describe our online and offline customer data practices. This information describes our practices related to individually identifiable customer data, not data that has been aggregated or anonymized. The data practices of Walmart's recently-acquired companies generally align with those of Walmart Inc. and Sam's Club. To the extent that there are substantive differences, they are noted in the discussion below.

Direct/indirect data collection (including from third parties): Walmart collects data to complete transactions and to provide services for our customers. The customer data we collect is also used to enhance the design of our customers' experiences in our stores, on our mobile apps, and online. For us, the purpose of data collection is to provide the best products and shopping experience to our customers, not to turn our customers into products.

The specific categories of customer information we collect, directly or indirectly, to better serve our customers include information we receive from our customers and information we receive from others:

- *Personal Information Provided Directly by Our Customers*—Our customers provide personal information directly to us, whether by creating accounts on our digital properties (*e.g.,* Walmart.com, Walmart Mobile App/Walmart Pay, Sam's

Club Membership), through transactions online, by shopping in one of our physical locations, or through other services we offer (*e.g.,* Auto Centers, Vision Centers, and Pharmacies).

- *Personal Information Provided by 3rd parties*—We also receive personal information about our customers from other sources to help correct or supplement our records, improve the quality and personalization of our services, and to detect, prevent and, investigate fraud.
- *Purchase/Transaction History*—When customers shop with us, whether online or in our stores, we collect data about their purchases and transactions not only to facilitate common retail functions like payment processing, product returns, and product recalls, but also to develop insights that will inform our efforts to make our customers' interactions with us easier and more enjoyable, and to let our customers know about other products and services they may want.
- *Health Care Data*—We also seek to help patients live healthier lives by using the data they provide to our pharmacies, vision centers, and care clinics. We use patient data to deliver treatment, payment, and health care services as well as to perform health care operations. The data is collected either directly from the patients or may be collected from their physicians, health insurance company, or others involved directly in their health care. Treatment and health care services include programs such as medication therapy management or prescription refill reminders. Health care operations include internal analytics and quality review activities. We collect, protect, and use this data in compliance with state and Federal health care privacy and security laws.
- *Browsing Information* —In order to provide a continuous and more personalized shopping experience, we use tools to collect browsing information, such as first-party cookies and web beacons to collect information about the use of our websites and mobile apps. From this, we can measure the effectiveness of our online customer interactions to help improve the customer shopping experience for future visits while also ensuring a seamless and pleasant experience during the current session. For example, this would allow our customers to shop on our website, leave to check another site, and then return to our site where they left off and continue their shopping experience. As a participant in ad networks, we allow third-party cookies on our website in order to provide our customers with a more personalized experience, where products are presented through more relevant advertising, and for website analytics.
- *Device Information*—When customers use our online sites, mobile apps, or other services, we may collect technical device information in order to provide our services. Examples of device information we collect include Internet Protocol (IP) address, the type of mobile device or browser used, a unique device identifier, and other information about a customer's session on our websites.
- *Location Information*—We are continually improving the in-store shopping experience to make it easier for our customers to locate products within the store. For example, when accessing Walmart.com from a desktop browser, we are able to use our customers' IP address to help them locate the nearest store. When customers enable location sharing through one of our mobile apps on their devices, we can provide information about the nearest Walmart or Sam's Club. Also, enabling location sharing allows customers to search a store's unique product inventory, locate departments and products within the store, and facilitate online grocery pick-up. Finally, we may be able to recognize the location of a mobile device in stores where we provide customers free WiFi access.

We do not sell or rent individually identifiable customer data to third parties. Under some circumstances, we may share individually identifiable customer data with third parties: (i) to help with our business activities, including fulfilling customer orders and processing payments through service providers like shipping or billing vendors, payment card processors, third-party delivery services, and our marketplace vendors; (ii) to offer optional third-party service or installation plans on the products we sell, and to offer co-branded products or services, such as a co-branded Walmart credit card; (iii) in response to a valid legal or law enforcement inquiry, subpoena or search warrant or for the protection and safety of customers; (iv) to help customers choose from a range of financial services products for which Walmart is an agent; or (v) with a customer's consent.

Some of Walmart's recent acquisitions share customer information, such as customer names, addresses, and e-mail addresses, with other companies for their own marketing and business purposes. These sharing practices are disclosed in the privacy policies of the Walmart acquisitions that participate in these practices, and customers can opt out of this sharing.

Data Usage: Aggregate and anonymized customer data provides us with insights to improve our services and products. There are also some instances where individually identifiable customer data is used to enhance these insights or provide our customers with a more personalized experience. For example, we use such insights to better communicate with our customers through e-mail, social media, and responses to surveys. Additionally, we use data about our customers' purchases to make it easier for them to quickly reorder frequently purchased items and personalize product recommendations.

Customer Access: Customers who have an online account can view the information they have provided to us online and also a record of their recent online transactions and purchases made in-store using Walmart Pay. Since the ability for the customer to view this information is tied to accessing the profile for the online account, customers without online accounts with us are unable to view similar information. Patients of our pharmacies, vision centers, and clinics have the ability to request copies of their medical records and may also request an accounting of how their Protected Health Information has been disclosed in accordance with applicable law. Beginning in January 2020, we will provide California residents with additional ability to request access to their personal information as specified under CCPA.

Advertising: Walmart uses customer information to offer advertising services to third parties. However, Walmart does not share individual customer's personally identifiable information as part of this business. We also allow third-party cookies on our website in order to permit our advertisers to provide our customers with a more personalized experience, where their products are presented through more relevant advertising.

The CHAIRMAN. Thank you so much. Ms. Richardson.

STATEMENT OF MICHELLE RICHARDSON,
DIRECTOR, PRIVACY AND DATA,
CENTER FOR DEMOCRACY & TECHNOLOGY

Ms. RICHARDSON. Chairman Wicker, Ranking Member Cantwell, thank you for the opportunity to testify today about Federal privacy legislation. CDT is a nonprofit tech policy organization that advocates for privacy, security, and free expression online. For 25 years we have supported a comprehensive Federal privacy law that cuts across all sectors and this hearing is evidence that Congress is closer than ever to accomplishing that. When we testified before you about a year ago, we asked that Congress pursue legislation that would do four things.

First, a law should shift the burden of privacy and security from users back onto companies where it belongs. To do that, it should have clear rules about the collection, use, and sharing of personal information in addition to any notice and consent framework. Second, a new privacy law should empower individuals to control their own data. Third, it should prohibit discriminatory uses of data and ways that harm underrepresented groups or disadvantaged groups. And fourth, a new law should build strong enforcement mechanisms that will be able to investigate and pursue violations of all these new requirements.

We are very pleased to say that between all of the bills before this Committee, we are substantially the way there. We have the right framework and the right principles, but we now need to stitch them together in a way that drives systemic change and how companies collect, use, and share information about us. Our written statement will address further details but today I would like to flag two things, one, corporate responsibility and two, enforcement.

First, corporate responsibility, especially for data use. What happens to data after a person consents to its collection? What are a company's continuing obligations after an individual signs up for a

product? How do we get to a world and a legal framework were opting in to use a product is just the beginning of a company's commitment to users instead of the end of it? The bill sponsored by the Committee members have made substantial headway here. For example, we are ecstatic to see that data security is now included in all of the major proposals, and that the leading Republican and Democratic bills recognize that civil rights and discriminatory data uses deserve special attention is a huge step forward for those who often bear the brunt of the most egregious practices online.

We know there are still disagreements about what the bills call minimization or loyalty to customers, and the questions beyond discriminatory uses, are there other data uses that are so risky they should be prohibited? How do we discourage some of the most offensive cases of over collection or surprising use of data and do so in a systemic way and not just on a user-by-user basis? To that end, we recommend the Committee be bold in this area.

Many of the components are already there. For example, bills by the Chair and Ranking Member mentioned necessity and proportionality, important concepts for scoping corporate behavior, and some of the bills also mentioned purpose limitations, an important concept for respecting the context in which data is first collected. One way to make these concepts exceptionally clear and operational on day one is to make a list of prohibited activities.

You could, for example, take some of these sets of sensitive data categories that are already in your bill, remove them from the opt-in regime, and say you simply just can't collect, use, or share them outside of the product that a person actually signed up for. We look forward to working with you on shaping that as it goes forward. The second topic I want to talk about today is enforcement, especially a private right of action. Much has been said about this topic being a make or break topic in the overall privacy debate. We would like to propose that the right solution probably lies somewhere between allowing individuals to sue over everything or sue over nothing. It is important to note that right now all 50-state unfair and deceptive practice laws include a private right of action.

These are the general purpose consumer protection laws that states could rely on to enforce privacy and security right now if they do not have a statute of their own. Some of them are very narrow, admittedly, but they do exist. And if our new Federal privacy law is essentially going to strike and replace these sorts of laws, we need to create a private right of action to keep consumers whole and ensure that they have at least as many enforcement options as they do now under State law.

Congress does have a lot of options here though. State and Federal laws are full of examples where legislators hemmed in litigation and directed it toward what they believed were really the most serious harms that consumers should be able to remedy. They include everything from the right to cure problematic behavior to letting Government agencies determine whether and how cases can go forward. This Committee should dig in and think about those sorts of controls that they could put on private rights of action to find a middle ground here for consumers and companies.

Thank you again for the opportunity to testify today. We are at an exciting moment where the public, Government officials, and

even companies have an interest in rebalancing our privacy laws to better favor people and we look forward to working with you to seize this moment and pass privacy legislation in 2020.

[The prepared statement of Ms. Richardson:]

PREPARED STATEMENT OF MICHELLE RICHARDSON, DIRECTOR, PRIVACY AND DATA, CENTER FOR DEMOCRACY & TECHNOLOGY

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to testify about comprehensive Federal privacy legislation. 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]

The Need for Comprehensive 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 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.

While the Federal Trade Commission's ability to police unfair and deceptive practices provide a backstop, large policy gaps 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.[2] 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.

Privacy and Data Security Legislation Pending in December 2019

Despite repeated criticism that Congress had not moved on privacy legislation, this Committee as well as other committees of jurisdiction have held meaningful hearings over the last year. The chair, ranking member, and several other Commerce committee members have introduced legislation on comprehensive privacy legislation or some piece of the bigger picture. Below are a number of key issues and discussion of how they can be addressed in legislation.[3]

Scope of legislation

Covered entities. It's crucial that any comprehensive privacy law cover all private sector entities that collect, use, and share personal information.[4] This includes not

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

[2] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583, 606–27 (2014).

[3] CDT focuses here on proposals authored by Chairman Wicker and Ranking Member Cantwell. CDT will have additional analysis on issues not addressed here, time permitting. Legislation by Committee members Thune, Blunt, Fischer, Blackburn, Blumenthal, Schatz, Markey, Klobuchar, and Peters all include important principles or language that can contribute to the final bill.

[4] We do not have a final recommendation as to whether HIPAA, Gramm-Leach-Bliley, FCRA or other existing consumer privacy laws should be reformed and made consistent with comprehensive proposals. CDT generally supports updating those laws, but Congress should move

only the prominent tech companies that have captured our attention recently, but also not-for-profit entities and the communication providers that are currently under FCC jurisdiction for privacy and security enforcement. Creating a single Federal standard will ensure that individuals can rely on the same baseline rights as they move across the digital ecosystem. To that end, Chairman Wicker's staff discussion draft[5] is one of the more comprehensive proposals.

We also recommend that legislation not categorically exempt small businesses.[6] They may collect, use, and share data in many of the same ways as larger entities.From the perspective of an individual consumer, the harms they experience are not mitigated because a company has fewer customers or makes less money. A privacy law that is clear and reasonable need not put an undue compliance burden on smaller entities, and many of the provisions in the bills authored by Chairman Wicker and Ranking Member already meet that test.

If the Committee feels that some procedural requirements are too much for a small business to comply with, legislation should adopt the Wicker staff discussion draft approach and exempt smaller entities from specific requirements. For example, it is more important that small businesses meet data security requirements, offer opt-ins, avoid discrimination, and provide access, correction, and deletion rights. It is less important that they conduct broader risk assessments, have certain staff members, or provide in depth reporting on their data practices.

Covered data. It is also important that legislation cover all personal data even if the Committee decides that there may be tiers of sensitivity that warrant different substantive requirements. We strongly recommend that the committee define covered personal information consistent with current FTC guidance which is best reflected in Ranking Member Cantwell's draft bill as "information that identifies, or is linked or reasonably linkable to an individual or consumer device, including derived data."[7] The additional qualifier that this data "can be used on its own or in combination with other information held by, or readily accessible to, the covered entity"[8] as proposed in the Wicker staff draft may be overly restrictive. Distinguishing between data that is linkable and that which is not serves two purposes. First, to discourage first parties from unnecessarily associating information with real people, but second, to offer down stream protections when information is shared with affiliates, third parties, or even in the instance of a data breach. These additional reasons for storing and using data in de-identified format will be frustrated by a definition that so heavily focuses on first party linkability.

Corporate Responsibility

The core of any privacy and security law must be corporate responsibility. While we should respect the rights of individuals to control their data, any systemic change will have to come from the entities that collect, use, and share data themselves. While a new law will have to regulate businesses of varying sizes, business models and data uses, there are some requirements that can be imposed across the board to ensure individuals receive digital civil rights that do not require them to micromanage the relationships they have with companies. All of the components of corporate responsibility are contained in the bills introduced in the Senate to date and only need to be stitched together to provide meaningful consumer protection.

Data use. Both Chairman Wicker and Ranking Member Cantwells' bills begin to address the exceptionally hard question of whether and how to regulate the use of data beyond any opt-in requirement. The FTC continues to develop a body of common law to prohibit certain data uses on a case by case basis, but a Federal privacy law can and should go one step further to categorically prohibit some of the riskiest data uses.

---

forward in the currently unregulated space if addressing financial services, health care and other sectors becomes an impasse.

[5] STAFF OF S. COMMERCE COMM. CHAIRMAN WICKER, STAFF DISCUSSION DRAFT (2019) available at: *https://aboutblaw.com/NaZ* (hereinafter WICKER DISCUSSION DRAFT).

[6] Pending proposals that define small businesses as those with a small number of users are more meaningful than previous iterations that focused solely on income or number of employees. These latter two metrics do not have a bearing on whether certain data harms will be deeply or widely felt by users. Ideally, a bill will borrow from the FTC's current guidance that focuses on number of users (5,000) and minimal data processing practices. FED. TRADE COMM. REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 15–16 (2012).

[7] Consumer Online Privacy Rights Act, S.___, 116th Cong. § 2(8) (2019) (hereinafter COPRA).

[8] WICKER DISCUSSION DRAFT, § 2(7).

Data use limitations exist to some extent in Chairman Wicker's minimization section[9] and Ranking Member Cantwell's loyalty section.[10] The committee could also borrow from legislation sponsored by Senators Blunt and Schatz on facial recognition technology[11] and Senator Markey's comprehensive privacy bill.[12] Ultimately, data use limitations must go beyond limiting data use to what a company *says* it will do with data, to creating an objective limitation regardless of what any one privacy policy entails. While there are a number of ways to craft this, a clear purpose limitation on sensitive data will make great strides towards aligning consumer knowledge and expectations with corporate behavior. To the extent that some provisions peg data use to what a company believes is a "reasonable" consumer expectation, they may be subject to bad faith arguments or protracted litigation about what exactly a "reasonable consumer" is.

Artificial intelligence and civil rights. Both bills recognize the importance of providing oversight of artificial intelligence programs and reinforcing longstanding discrimination laws that may be undercut by current data practices. Despite their differences, we hope this signals a commitment to addressing these issues in any final privacy and security legislation. CDT prefers the breadth and depth of Ranking Member Cantwell's approach and looks forward to working with the committee on refining these requirements as necessary as the legislation moves forward.

Data security. CDT commends Chairman Wicker and Ranking Member Cantwell for including data security requirements in their draft bills. Close to half of U.S. states do not have a general purpose data security law, and FTC enforcement under its Section 5 authority will always be limited to what its resources allow. We recommend combining the two and adding one additional provision.

First, the committee should adopt Chairman Wicker's base text in section 204 regarding the requirements of a reasonable data security program. Second, the committee should adopt Ranking Member Cantwell's scoping of data to be covered. Her draft protects not only sensitive information, but all personal information. Because both bills impose a reasonableness standard that will peg to the size and complexity of the organization and the sensitivity and use of the data, it is unnecessary to exempt certain data sets from the overall security requirement. Third, this section should provide overall rulemaking for the FTC. Right now, the Wicker and Cantwell bills require guidance or limited rulemaking, but it is time for the longstanding guidance of the FTC to be written into regulation. To the extent that some in the corporate sector have criticized the FTC's data security requirements as too vague despite long-standing guidance in this space, they will benefit from having regulations on the books to better describe requirements.

Individual rights

Both the Wicker and Cantwell drafts offer meaningful individual controls to individuals and we commend the comprehensive approach contained in them.

Opt in requirements for sensitive data. Both bills include a comprehensive list of sensitive data that is subject to affirmative, express consent. The differences are minimal but the definitions should be amended in a few key ways. First, the committee should adopt an expansive definition of health information, and we recommend borrowing from CDT's model legislation[13] which incorporates not only data that reflects a person's mental and physical status, but data that is processed for health or wellness purposes. As Senator Klobuchar and Murkowski recognize in their Protecting Personal Health Data Act,[14] apps, wearables, and devices are creating and collecting intensely personal information that can be used in ways that greatly affect a person's mental and physical well-being. Any definition should ensure that these resulting data sets receive heightened protection.

Second, sensitive data should include Ranking Member Cantwell's formulation of "information revealing online activities over time and across third-party website[s] or online services."[15] This formulation is meaningfully different from the type of data that will be regulated by "Do Not Track" functions the FTC would facilitate under either proposal.[16] We understand this to mean data collection that is more pervasive and intrusive than first party tracking or one-off identification of an indi-

---

[9] WICKER DISCUSSION DRAFT, § 105.
[10] COPRA, § 101.
[11] Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. § 3 (2019).
[12] Privacy Bill of Rights Act, S. 1214, 116th Cong. § 3 (2019).
[13] CTR. DEMOCRACY & TECH., CDT FEDERAL BASELINE PRIVACY LEGISLATION DISCUSSION DRAFT, § 1(2) (2018). *https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.*
[14] Protecting Personal Health Data Act, S. 1842, 116th Cong. § 2 (2019).
[15] COPRA, § 2(20(J).
[16] COPRA §, 105(b); WICKER DISCUSSION DRAFT, § 104(a–b).

vidual which arguably deserve less protection. This formulation is also consistent with Senator Blackburn's BROWSER Act[17] which has long recognized the unique place at which edge providers sit in the ecosystem. While all entities should play by the same set of rules, recognizing that long term tracking of this data is particularly risky for privacy and security is consistent with the overall approach of the bills.

Product development exception. In general, the list of exceptions to the opt-in right contains reasonable data use that is core to offering the product an individual signs up for. They fairly recognize that some data processing is absolutely necessary to offer safe and effective products and cannot be opted out of either individually or at scale. However product development as listed in Chairman Wicker's staff discussion draft is meaningfully different from the rest of the data uses. It permits companies to collect data without someone's consent even if they have no understanding of how it will be used or whether they will benefit from the use at some point in the future. Since product development is solely for the benefits of the companies who collect the data—unlike everything else on this list of exceptions—it should not be done without an individual's consent. To the extent the Committee does not want to inhibit innovation, it should further explore why the de-identification carve out is insufficient for product development, and whether some middle ground should be created for processing data this way.

Access correction deletion portability. The individual controls are comprehensive. Our only suggestion is that the Committee include the timelines drafted into Wicker's staff discussion draft to ensure that rights are afforded on a reasonable timeframe.[18]

Data broker registry. We commend the Wicker staff draft for including a data broker registry housed at the FTC.[19] A registry will ensure that individuals can discover and exercise their rights against data brokers who have amassed incredible amounts of sensitive data on the average American. While many of the provisions in both the Cantwell and Wicker drafts may slim down the amount of information that eventually ends up in data broker databases, these entities are likely to continue collecting information and will still be holding data that has been accrued over decades of largely unregulated data use. That someone can exercise their access, correction, and deletion rights against these entities is the best protection against future data abuse.

Enforcement

Both Chairman Wicker and Ranking Member Cantwell's drafts include meaningful enforcement mechanisms, but they differ in a few important ways.

First, Ranking Member Cantwell includes a private right of action ("PROA") for all violations of the law.[20] CDT believes a targeted private right of action is necessary for meaningful enforcement. This is not only because the number of entities that will be swept under new regulations will necessarily dwarf the resources of the FTC and state attorney generals, but because our history is full of instances where government actors simply did not have the wherewithal to be first movers on important social issues. Because private litigation has served such an important function in civil and consumer rights enforcement in the past, it should be reserved in some form in Federal privacy legislation.

It is important to note that all 50 state unfair and deceptive practice laws include some form of a private right of action, even if substantially limited.[21] If a privacy bill seeks to categorically move privacy and data security out of these laws,[22] it should ensure that consumers are at least equally positioned to defend their rights as they are now.

The proper balance likely lies between the Cantwell and Wicker drafts in a specific delineation of what provisions can be enforced by PROA and under what condi-

---

[17] Balancing the Rights Of Web Surfers Equally and Responsibly Act of 2019, S. 1116, 116th Cong. § 2(12) (2019).

[18] WICKER DISCUSSION DRAFT, § 103.

[19] *Id.* § 203.

[20] COPRA, § 301(c).

[21] CAROLYN CARTER, NAT'L CONSUMER LAW CENT., CONSUMER PROTECTION IN THE STATES: A 50–STATE EVALUATION OF UNFAIR AND DECEPTIVE PRACTICES LAWS 32–46 (2018).

[22] While California has a general purpose privacy law, and some states have targeted regulation like Illinois' Biometric Information Privacy Act, privacy law is overwhelming homed in state UDAP statutes at present. Similarly, roughly half of states do not have express data security requirements, so enforcement against unreasonable data security falls under UDAPs too. NAT'L CONFERENCE OF STATE LEGISLATURES, DATA SECURITY LAWS: PRIVATE SECTOR (May 29, 2019) *http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.*

tions. State and Federal laws are full of examples where PROAs are crafted to limit litigation to the most important harms. We recommend that the Committee consider this approach to find the right way to maximize accountability and minimize nuisance litigation. Such litigation controls could include opportunities to cure, harm requirements, reduced or nonexist damages or prior agency review, for example. We look forward to working with the Committee further on finding the right way forward on PROAs.

Second, legislation should allow state attorneys general to bring cases in state court and should not force consolidation of cases into the D.C. Circuit. Courts at every level are backlogged and funneling enforcement into too few courts will greatly delay meaningful defense of consumer rights.

Conclusion

CDT thanks the Commerce Committee for the opportunity to testify about privacy legislation today. We are encouraged by the many thoughtful proposals already introduced in the Senate and believe that passing a single comprehensive privacy and security law should be a priority for committee action in 2020.

The CHAIRMAN. Well, thank you to all five of you for some very good testimony and some, I think, very helpful suggestions. Let's get right to some of the unresolved issues between my draft and the Ranking Member's draft. And so, let me just pick up with you, Ms. Richardson. Your group issued a draft privacy legislation last year that does preempt State data privacy laws. Why did you do that? I think everyone can see how that is a benefit to private industry, retailers, convenience stores, Internet service providers, technology companies. How does it benefit consumers to have a nationwide standard?

Ms. RICHARDSON. So, I think there are a couple of things here. One is that the first privacy bills we are seeing at the State level are not very comprehensive. The law in California for example is both historical, we want to recognize that, but it is not complete. It is mostly an opt-out law and many of the proposals before the Committee now are actually stronger. So there is an opportunity here to actually do better than what we are seeing at the states.

But second, I want to point out it took 15 years for all 50 states to eventually pass breach notification and that is a very narrow issue. I am concerned that if we have to go state by state to cover everyone in this country with a privacy law, we are going to be on the next version of the internet. So there are benefits to consumers if we can get a really high standard at a Federal law now.

The CHAIRMAN. Ms. Ohlhausen, how would this benefit consumers nationally?

Ms. OHLHAUSEN. So, as it has already been mentioned, consumers' rights need to be clear. They need to understand them, and they need to know how to enforce them. And having a uniform Federal standard will allow consumers wherever they are in the U.S.—you know, the Internet is as an interstate entity, wherever they are purchasing, wherever they are transacting or engaging in a service, those same rights will follow them.

So I think that gives them an enormous benefit to now have with a detailed comprehensive set of rights like both of your proposals or the numerous proposals provide that this will allow the consumers wherever they work, wherever they travel, wherever they are transacting business to understand what those same rights are and to have them available to them.

The CHAIRMAN. OK. Ms. O'Connor, Ms. Richardson believes that the proposals that I have outlined and Senator Cantwell and some

of her colleagues have put forward are much stronger than the California law. I agree with that. Do you agree with that? And it is important to note that the California legislature looked at amending their law, chose not to expand the private right of action, for example. So could you please comment on those issues?

Ms. O'CONNOR. Thank you so much for that question, Senator. In fact, we are scrambling to be ready for the January 1 compliance date at Walmart in California. And to echo what has already been said, simply adding more complexity to consumers' lives is not actually I think helping their privacy. There is strength in clarity, simplicity, and consistency that could be offered at the Federal level.

If a consumer in one state is certain that they are going to get the same rights and same value from their data that a consumer in another state—let me give you an example actually. On Thanksgiving weekend, I sent my sister the Woodwick Frasier Fir Candle. It is a great little candle. I recommend it highly. It is on *Walmart.com.* It is green. It is a perfect holiday gift. It makes a little crackling sound. She lives——

The CHAIRMAN. How much was it?

Ms. O'CONNOR. It was $24.99. Thank you—for the oval shape. It is great. I bought four of them for myself, only one for her, but that is another story. She lives in New Jersey. I purchased it on *Walmart.com* using my cell phone within the 516 New York area code. I live in Maryland. It is shipped from—I don't actually know which warehouse. We are based in Bentonville, Arkansas and our e-commerce site mostly use—our service out of California. Which State law applies to that transaction? Whose data is going to be protected? Her data, my data, the transaction data? Where does it happen? This is not helping our consumers' understanding, our average everyday consumer transactions, simplicity, efficiency, and speed.

So I have always believed, in all of the roles I have had in the four privacy officer roles I have held in the private sector and two in the Federal Government and my time in civil society, that a comprehensive Federal standard is the right answer for the American citizen.

The CHAIRMAN. OK. Well, we have a lot of issues to get to, but thank you very much, and my time has expired.

Senator Cantwell.

Senator CANTWELL. Thank you, Mr. Chairman. Again, thank you to the witnesses. I am going to try to go fast because there is so much to cover but all your testimony was so helpful. I just want to clarify if I could just on quick yes-no answers, if you do believe in a consumer privacy rights writ large, that we should say that their rights and that those rights should be enforced somehow depending on how? Just say yes.

Ms. BRILL. Yes.

Ms. OHLHAUSEN. Yes.

Ms. MOY. Yes.

Ms. O'CONNOR. Yes.

Ms. RICHARDSON. Yes.

Senator CANTWELL. OK. And several of you mentioned harmful data practices are people for specifying the harmful data practices

and that consumers should be protected against harmful data practices?

Ms. BRILL. Yes.

Ms. OHLHAUSEN. Yes, with an understanding that consumers, you know, may have different preferences.

Ms. MOY. Yes.

Ms. O'CONNOR. Yes.

Ms. RICHARDSON. Yes.

Senator CANTWELL. OK, go back. Ms. Ohlhausen, what do you—different preferences? Either there is harm—I mean harmful has to be determined, right?

Ms. OHLHAUSEN. Harmful has to be determined, but for example at the FTC when we did look at things like substantial injury did the consumer, or could the consumer have avoided it? Consumers can sometimes make different types of choices where I may not want to share information, but someone else, my neighbor may feel more comfortable sharing that information. Having an understanding that consumers also may have somewhat different preferences.

Senator CANTWELL. OK, let's go to something maybe a little harder and I apologize Ms. O'Connor. I should have come up with some—my team should have come up with somebody that wasn't here today. But on Walmart, this is just an example, we all know that people put up a general privacy statement. They basically say something like—well, actually I saw a statistic like that. I don't know what it was, 70 percent of companies now share data with third parties, and it is just standard part of their privacy statements.

But on your website, I think you have a privacy statement that basically says, yes, information might be shared. But now with Ghostery you can actually see—just hold it up Melissa. Just hold it up. Ghostery can now show you an actual tracking of how many different people are tracking that data. So 19 different advertisers are taking that data that you generally said here is what is, you know, in our privacy statement, which you have to read.

OK, but now we know by using that app that 19 different people were tracking that data and information. So our concept, at least my colleagues and I here are saying, you should be more upfront about that. That is just a little too vague on what is happening to information and data. So where are the witnesses on what we should do about this so that there is clarity to consumers?

Ms. BRILL. Yes, so this is actually a really important question, and of course the California law focuses on giving users the ability to opt-out of sharing with third parties. And a number of the proposals that various committee members have pulled together also focus on what is happening with respect to sharing with third parties.

Senator CANTWELL. OK. I am going to run out of—so, do you think we should be more explicit with consumers than just we are sharing information with a third party? Do you think they should list the names or list the companies, or what data is being shared so that——

Ms. BRILL. So I think focusing only on third—forgive me for interrupting. I think focusing only on third parties is not business

model neutral and will have competitive effects that are unintended but will be severe.

Ms. OHLHAUSEN. We are in favor of increased transparency for consumers but in a way that is not overwhelming. So if they want more details they can get it or if they just need general types of third-party sharing that would also be available.

Ms. MOY. I do think third-party sharing is a huge problem. And it is impossible for consumers really to know where their data is going. I think one of the things that I see in the draft bills is that the rights, when consumers exercise their rights, those rights would have to be communicated to additional parties and exercised by them, and I appreciate that.

Ms. O'CONNOR. Thank you so much, Senator, and thank you for using our website, which actually we are very proud, and we have worked on. I have a tremendous team in Bentonville and in San Bruno in Sunnyvale, California. Most of what you saw in your ghost research is likely online tracking that we do of ourselves to see who is coming to the website, how long they are staying, better service you on a return visit so that as you probably note when you leave and you have got something in your basket, it should hopefully still be there when you return. I don't believe any of those, and I will certainly follow up with your team and staff and my staff as well, are sharing personally identifiable data about our customers. And let me be just really clear, we do not sell or lease personally identifiable information about our customers outside of the Walmart family.

Senator CANTWELL. Well, and we want to hear from Ms. Richardson about whether this is the practice writ large that we have to get to figure out what we can do and what consumers are doing—Ms. Richardson, I think I know your answer because you said in your testimony, you should just be able to say no, don't do this.

Ms. RICHARDSON. Yes. We would support limitations on third-party sharing.

Senator CANTWELL. Thank you. Thank you, Mr. Chairman. I could go into a bunch of AI questions, which I really have, because I really do think that what we are discussing today is really, really important. But I guarantee you tomorrow's challenges are going to be much more significant and we have to figure out how to get something in place to help us deal with that for the future. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cantwell.

Senator Thune.

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

Senator THUNE. Thank you, Mr. Chairman, for holding today's hearing. As members of this Committee continue to work on crafting a national consumer data privacy bill, it is my hope that we can ultimately work together on a bipartisan basis to produce legislation that puts consumers interests first while still allowing the private sector to innovate and grow the economy.

I think all of us understand, or at least should, that only a bipartisan proposal has a chance of clearing the Senate and becoming law, and in my view, that bipartisan outcome must include strong

consumer protections while also avoiding the regulatory patchwork that is beginning to emerge at the State level.

I remain committed to working with the Chairman, the Ranking Member, and our colleagues on both sides of the aisle to find a consensus solution. Since we started privacy discussions last Congress, I have said the consumers are entitled to clear and concise explanations of how the services they use are collecting and using their data.

In one specific area where I believe consumers deserve more transparency and control is with respect to how Internet platforms use artificial intelligence and opaque algorithms to make inferences from the reams of data collected about all of us that too often result in users being caught in a so-called "filter bubble."

The filter bubble is essentially the unique universe of information generated on an Internet platform for each user. Many users are unaware of the filter bubble. That is why I have introduced the bipartisan Filter Bubble Transparency Act which would give individuals a greater understanding of how Internet platforms use algorithms to increase user engagement.

You would also give consumers the option to engage with a platform without being manipulated by opaque algorithms powered by the user's own personal data. And I am proud to have Senators Blumenthal, Moran, Blackburn, and Warner as co-sponsors of this bill. At the same time, whether it is algorithm transparency or privacy, I understand that bills touching on highly technical issues can have potentially unintended consequences. So I welcome constructive feedback on this bill and the Committee's efforts more generally.

I would like to ask, if I might, a couple of questions relating to transparency on Internet platforms as well as the larger privacy debate. And the question for each of you is regarding the Filter Bubble Transparency Act. It is more of a general question, but you would agree that it is appropriate to give consumers more information and choice about how sophisticated algorithms and artificial intelligence are often selecting what the consumer sees on Internet platforms? And I would just like it if you can quickly comment on that.

Ms. Brill.

Ms. BRILL. We think it is a very important issue. We are very grateful that you have raised it and we look forward to discussing it with you further, how this could be implemented.

Ms. OHLHAUSEN. We are certainly in favor of giving consumers more transparency about how their data is used and how that shaped what they see.

Ms. MOY. I absolutely think so. I think you know—and many platforms optimized for engagement and that optimization can have unintended consequences. One of those certainly as you mention is the filter bubble which drives political polarization. We also see this driving the spread of misinformation and disinformation and also discriminatory advertising. And for all of those reasons, I think we need action on this issue.

Ms. O'CONNOR. Yes, Senator, we are supportive of the intent of the bill.

Ms. RICHARDSON. Yes, we support the more transparency and accountability for how AI is used.

Senator THUNE. OK. Ms. Brill, Ms. O'Connor, aside from California at least a dozen other states are in the process of enacting consumer data privacy laws. What impact would a diversity of State privacy laws have on your respective companies? And then as a follow up to that, apart from the compliance challenges for companies, are there concrete benefits for consumers to having a common national standard, assuming that it is robust?

Ms. BRILL. Thank you for that question. Microsoft believes that we do need robust privacy laws in the United States, including laws that will be protective of consumers and provide greater consumer rights as well as greater responsibilities on companies. To the extent that states are enacting laws, they are I believe spurring a great conversation in the United States about the need for more privacy protection.

So we applaud what the states are doing. Having said that, at some point in time, if we do have 50 State laws that start to conflict, it might be one thing for a company like Microsoft to be able to comply with it, but many, many of our customers and millions of other companies might have much more difficulty. So conflicting State laws could end up being problematic down the road, but we do applaud the states for the work that they are doing because we so desperately need privacy legislation in this country.

Ms. O'CONNOR. Thank you, Senator. I would certainly echo what has already been said and simply note that a complexity of State laws can have a chilling effect on the consumers' comfort level with a company with which they are doing business. They could have greater certainty and clarity and understand the transactions that they are entering into with a single Federal standard. Our customers shop across state lines not only on the Internet but in the physical world as well, and we want them to be protected wherever they shop.

Senator THUNE. Thank you, Ms. O'Connor. My time is up. I would ask consent that I be able to have a letter included in the record from the Privacy for America Coalition.

The CHAIRMAN. Without objection.

[The information referred to follows:]

PRIVACY FOR AMERICA
December 3, 2019

Hon. ROGER WICKER,
Chairman,
Senate Commerce Committee,
Washington, DC.

Hon. MARIA CANTWELL,
Ranking Member,
Senate Commerce Committee,
Washington, DC.

Dear Chairman Wicker and Ranking Member Cantwell:

Privacy for America[1] applauds your leadership for holding this week's hearing and your ongoing interest in protecting consumer data privacy. We share your interest and want to bring to your attention that, today, Privacy for America released a comprehensive new framework for nationwide privacy legislation that would fundamentally change the way consumer privacy and security are protected in this

[1] Privacy for America is a coalition representing industry, including the advertising industry, with members from virtually every sector of the economy. The steering committee includes leaders from the 4A's (American Association of Advertising Agencies), ANA (Association of National Advertisers), Digital Advertising Alliance (DAA), IAB (Interactive Advertising Bureau), and NAI (Network Advertising Initiative).

country. We hope the framework, which expands and builds upon principles released in April, will advance policy discussions and help build the consensus necessary to enact bipartisan data privacy legislation this Congress.

The framework represents a new approach to data privacy that would not rely on the current 'notice and choice' model, which presents consumers with endless and complex privacy notices that they are essentially forced to accept if they want to participate in today's economy. Instead, this new approach clearly defines and would make illegal data practices that would harm consumers or otherwise make personal data vulnerable to breach or misuse, while preserving the benefits that come from the responsible use of data and ensuring the economy can grow and innovate. This new paradigm shifts the burden away from consumers and toward a common set of privacy norms, backed by strong enforcement to ensure accountability by the businesses and organizations that use data every day.

This framework offers a detailed new approach with robust protections for consumers and clear penalties for companies that do not comply. In addition to enumerating prohibited data uses, Privacy for America's new paradigm includes several additional provisions that together constitute a comprehensive privacy framework. Among the framework's provisions are:

- Prohibitions against using consumer data to determine eligibility for a job, health care, financial aid, insurance, credit or housing outside of existing laws governing eligibility for these important benefits;
- Prohibitions against discrimination by using consumer data to set higher prices based on an individual's race, color, religion, sexual orientation, and more;
- Prohibitions against using sensitive information like health, financial, biometric, and geolocation data without first obtaining users' express consent;
- Provisions protecting so-called "tweens": a vulnerable group of consumers over age 12 and under age 16 that is actively engaged online but not often subject to constant parental oversight;
- A requirement that companies make privacy policies much easier to read and understand;
- Provisions that give consumers the right to request access to and deletion of the personal information that a company holds about them, as well as the right to port certain data from one platform to another;
- Individuals can choose to limit companies' use of personal information to draw detailed inferences or make predictions about them, with certain exceptions; and
- Significant new rulemaking authority, resources, and staff that will allow the Federal Trade Commission to more aggressively pursue and punish bad actors, bolstered by enforcement by state attorneys general.

Again, Privacy for America applauds your leadership, and we look forward to continuing our work with you and other leaders in Congress to see comprehensive Federal data privacy legislation enacted.

Sincerely,

STUART P. INGIS,
Counsel,
Privacy for America.

cc: All Members of the Senate Commerce Committee

Senator THUNE. Thank you.

The CHAIRMAN. Senator Blumenthal, you probably don't have any questions——

[Laughter.]

Senator BLUMENTHAL. Thank you.

The CHAIRMAN. Am I incorrect there? Senator Blumenthal.

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

Senator BLUMENTHAL. Thanks. Mr. Chairman, and thank you for having this hearing, and thank you to our Ranking Member as well. We have a lot of bills, but we have no Federal law. I want a law. There will be more bills, and I can tell you, may be no sur-

prise to any members of our panel, but here is a bulletin from outside the beltway. People are angry and scared more than ever before and they don't care whether it is a Federal law or a State law. They want a law. And you will see State laws all around the country.

Hopefully, they won't create too much inconsistency, but that is where we are going if we fail to act. And the reason that they are angry and scared is that they feel rightly this data belongs to them and they are losing control over it. They want that control back and they want a means of enforcing the law.

I agree completely with my colleague Senator Cantwell in emphasizing enforcement. That was pretty much my professional career for all the years that I was a prosecutor and trial lawyer before I came here. And I believe strongly in private Attorneys General even though I was an Attorney General before I came here. We know that consumers should be able to protect their rights in court when State or Federal agencies fail to do it for them.

So let me ask Ms. Moy and Ms. Richardson, do you agree that if we preempt State laws and create this Federal standard, that we have to allow private enforcement to ensure that the Federal standard provides the remedies that they have under those laws?

Ms. MOY. Absolutely, and I would say that there needs to be some agility mechanism too to continue updating the standards.

Ms. RICHARDSON. Yes. We recommend it would be targeted at the most important offenses though and material harms, but yes, we would support one.

Senator BLUMENTHAL. And let me ask all the members of the panel. I am assuming that you would agree with me that any Federal law should add to the rights that consumers have, enforceable rights, not take them away. Anybody disagree? And that means for example in the California law and the Illinois law where there are private rights of action, we should preserve them in some form. Correct? Everybody seems to agree?

Ms. Brill.

Ms. BRILL. The California private right of action is actually a fairly limited private right——

Senator BLUMENTHAL. It is a limited one, but still we don't want to take it away, we want to add to it.

Ms. BRILL.—I do believe in a Federal law. We need to focus on consumer redress, and I think there are lots of ideas about how to do that. I am not certain that I would agree that all of those mechanisms that exist in all the states should be added upon in a Federal law.

Senator BLUMENTHAL. Would you agree that there should be some provision for injunctive relief to stop ongoing harm?

Ms. BRILL. Yes. I do think that injunctive relief of having individuals have the ability to obtain injunctive relief is important. I also think it is important to require companies to have a process internally so that if someone is seeking their data or wants to delete it or correct it and they are not satisfied with the initial decision about that access right, they have ability to escalate that within the company as well. An administrative process, if you will.

Senator BLUMENTHAL. And I hope that you and other members of the panel would be willing to work with the Committee to devise a standard that preserves that kind of right.

Ms. BRILL. Absolutely. I look forward to working with the Committee on that.

Senator BLUMENTHAL. I would like to ask Ms. Moy and Ms. Richardson, is the FTC really likely to bring a lawsuit in the majority of consumer complaints that deserve action? Would you want to trust only the FTC?

Ms. MOY. I think it would be really problematic to rely on the FTC alone. If you look at the very strong, or the strong, children's privacy law that we have, COPPA, that law has been in existence for over 30 years and there have been only—I am sorry, over 20 years, and there have been only 31 enforcement actions in that time. And in that time, some of those that have violated it, violated it for years before an enforcement action was brought.

And that is because we are talking about an agency that really only has 40 people working on these issues. That is not enough. And as I said before, if a State AG is only able to bring—you know, the California State AG which has a large staff was only able to bring three or four privacy prosecutions a year, we are going to need a greater force multiplier than that.

Ms. RICHARDSON. I think that is correct. There are going to be so many new entities swept under this law and new rules that enforcement and clarifying exactly what is expected of companies is going to take a lot of actions. And there is just going to be cases where small groups of people are affected in small states that will never become a national enforcement priority. And that is where State AGs need to be able to protect their own constituents.

Senator BLUMENTHAL. My time has expired, but I just want to thank all of you for being here today. And I do want a law not just a bill, and a law isn't going to happen unless it is bipartisan. That is why I am working with a number of my colleagues, most prominently Senator Moran, and we have been for some time. These issues are not easy, but we have a responsibility to address them. Thank you, Mr. Chairman.

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

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

Senator FISCHER. Thank you, Mr. Chairman. It might not be the most exciting but a key consideration as we look to the data privacy really, I think, comes down to definitions. The nuances and defining covered data and what constitutes data collecting, selling, and processing all have major impacts for industry and consumers alike.

Ensuring these are clear and consistent in U.S. law will be fundamental to a unified Federal privacy framework. Commissioner Ohlhausen, if we were to multiply definitional differences by up to 50 states and force companies to map out which states have the same terms, similar terms, or dissimilar terms, what does that potential world of compliance look like?

Ms. OHLHAUSEN. Thank you, Senator, for your question. I think that it is a world that is very confusing for consumers, and it is costly and confusing for companies as well to know what their obligations are and how to comply with them across many, many hundreds of definitions for similar behaviors.

Senator FISCHER. In particular, how would this affect any new entrants into the market who are looking to innovate? Wouldn't it be closed off almost?

Ms. OHLHAUSEN. Right. Absolutely. It is one of the things that we have seen documented post GDPR. While GDPR certainly has some very good provisions, it has affected small and medium enterprises who are not able to comply and who have just simply withdrawn from the market.

Senator FISCHER. Do you think that the friction of these differences could possibly help serve to further entrench our big tech companies?

Ms. OHLHAUSEN. Absolutely. In anti-trust terms we call it raising rivals' cost. It can be away for—a path for big companies who have the resources, who have access to, you know, lawyers and people to do all of this for them. They have an advantage.

Senator FISCHER. A lot of times when we talk about the importance of consent for consumers, we do have to center on data privacy, and the legislation that we have seen from both the Chairman and the Ranking Member, there is language that both products seeking to ensure that affirmative express consent—and that is clearly given.

However, too often we have a lot of online platforms that are manipulating how users interface and that weakens that consent product. Users are going to see a false choice that is presented to them on the screen and they press the "I agree" button. These scenarios hide what the action actually does such as accessing your contacts, your photos, your location, your messages, your web activity, on and on.

Commissioner Brill, can a privacy framework involving consent function effectively for consumers if it also does not ensure that UI design presents fair and transparent options to manage personal data settings?

Ms. BRILL. Thank you so much for the question, Senator. It is very important that to the extent that consent is required that it needs to be surfaced to users in an immersive and very easy mechanism so that consumers can really understand what their choices are and have real choices.

Of course, consent is an important component of any privacy law, but requiring only consent or relying on only consent really places much too much of a burden solely on individuals to govern privacy in this country, which is one of the reasons why we think it is very important and we applaud all of the work on both sides of the aisle to build into the draft frameworks that we are looking at a focus not just on consent and choice by individuals, but also placing real responsibilities on companies to ensure that they are using data responsibly and appropriately.

Senator FISCHER. I have introduced a bill with Senator Warner, The Detour Act, which Microsoft has been supportive of and I thank you for the input and the feedback that we received on that.

Do you think that we have to have a Federal data privacy vehicle that would address this issue as well, to be able to get the Detour Act as part of that, that that is going to be necessary, I think, to really have a direct benefit that consumers will see immediately?

Ms. BRILL. It is a very important issue and we look forward to working with you on how to build those concepts into whatever vehicle moves forward. Absolutely.

Senator FISCHER. Thank you very much.

The CHAIRMAN. Thank you, Senator Fischer. I would at this point remind Members that we have a series of three votes beginning at 11:30 a.m., three cloture votes. And what we are going to try to do is just continue the question and answer as Committee members alternate back and forth.

Senator Schatz.

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

Senator SCHATZ. Thank you to all of the testifiers. This has been a great hearing so far. I want to zero in on something Senator Fischer was talking about which is notice and consent and choice and the ability to opt out. Now, here is my view. My view is that consumers effectively have no choice because: (a) they are going to be asked to make these choices, to agree to privacy policies multiple times in a day; (b) these things are just too long. They take 10 minutes to read.

I think the Facebook policy takes an average of 18 minutes to read. And then finally, an educational attainment requirement of college plus. I think the Airbnb policy has a readability score that requires the educational attainment equivalent of a doctor or a lawyer and it takes 10 minutes to read. And then I will just add one final thing which is in an IoT universe and an AI universe, we have got multiple sensors pinging off of your body, your phone, your wrist, and everything else.

The idea that you are going to daily opt out of the world is preposterous. So I will just start with one very simple yes or no question, and I will start with Ms. Brill and move down the line. Do you think that Facebook and Airbnb users know how their data is being used?

Ms. BRILL. Without focusing on any particular company, I think navigating the current ecosystem of privacy statements is very difficult and we need more immersive——

Senator SCHATZ. I will take that as a diplomatic no.

[Laughter.]

Senator SCHATZ. Ms. Ohlhausen, in the interest of time, I will take a no.

Ms. OHLHAUSEN. Right. I think that——

[Laughter.]

Ms. OHLHAUSEN. I think that most users probably don't, but some do, and some people who are very immersed in this do surface problematic privacy provisions.

Senator SCHATZ. Sure. Ms. Moy.

Ms. MOY. No.

Senator SCHATZ. Ms. O'Connor.

Ms. O'CONNOR. Senator, we completely agree with the concept of a duty of loyalty that you so eloquently in imply in your drafts. You heard it in my original testimony. We feel like we have a duty of care to our customers in all sorts of ways. So, and I am sorry to go on, but I think once called myself the Mark Twain of privacy policies because I have written more words that nobody has ever read online and offline, so I think in the interest of our busy working families that our customers, we need to be efficient and clear in our disclosures.

Senator SCHATZ. Thank you.

Ms. RICHARDSON. I will just say no.

Senator SCHATZ. Thank you very much. So, do you—just down the line. I will start with Ms. Richardson. Do you agree that a strong privacy law must prohibit companies from using the data that they collect in ways that harm users?

Ms. RICHARDSON. Absolutely. I think when we look at Mr. Wicker's bill and Ranking Member Cantwell's bill, they are the gold standard of what consent looks like when it works right, but where we could do more is buildup the other side of that equation and put more obligations on companies.

Senator SCHATZ. Right. This is belt and suspenders. I mean part of the reason for a duty of care and a duty of loyalty is the difficulty of empowering consumers as a practical matter. The other part of this is that it is impossible, even with all these smart people, to enumerate and specify and ban future bad actions 15 years from now when this statute is still hanging over an IoT and AI universe, and we don't know what kind of bad stuff companies are going to do. It is going to be very difficult to predict them in a bill that we are going to write next year. I am sorry, who am I on? Is it Ms. O'Connor? Thank you.

Ms. O'CONNOR. I think you were looking for a yes.

Senator SCHATZ. Yes.

Ms. MOY. Yes. I agree completely. That is why I would appreciate that at least some of the drafts have rulemaking authority for unfairness—I am sorry, for harmful data practices as well.

Ms. OHLHAUSEN. Drawing on the FTC's unfairness standard which looks at substantial injury but also balances it with consumers' ability to make these decisions as well if they have the right amount of information, I think that is a useful model to look to for any legislation.

Senator SCHATZ. Thank you.

Ms. BRILL. Yes, and we are deeply encouraged by the fact that both drafts on both sides of the aisle have concepts around avoiding harm, and that is very important.

Senator SCHATZ. Ms. Brill, I want to stay with you for a moment and talk about the FTC's authorities. First, fine authority, rulemaking authority, and staffing. Can you give us your quick recommendations there?

Ms. BRILL. We need first-time fining authority. I believe rulemaking authority is important, especially as these bills are going to be complex, and in the United States many of these concepts will be brand new and millions of companies will need more guidance. So I think rulemaking authority guidance workshops are all going

to be very important. And staffing, couldn't agree more that the FTC is deeply understaffed in this area in particular.

Not only are the British data protection authorities and the Irish data protection authorities much better staffed, but if you look across Europe, it is hundreds of people in each country dealing with privacy issues. We definitely need many, many more people in the FTC and also more technical expertise. They have technical expertise. They are great, but we need to build that up.

Senator SCHATZ. Thank you.

The CHAIRMAN. Thank you, Senator Schatz. Senator Moran.

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

Senator MORAN. Mr. Chairman, thank you. Thank you to the Ranking Member for having this hearing and thank you to our panelists for joining us. Ms. Brill, thank you for the time you spent with me and my staff yesterday. I will start with you, Chairman Ohlhausen. Hello. Nice to see you again. With the recently adopted California Privacy. Act, Consumer Privacy Act, which was slated to take effect, is slated to take effect this year, this next year, I assume we would agree that it is going to influence what other states will do and there is concern expressed by some, many about a patchwork of standards across 50 or more states.

How are—the California law preempt municipalities like San Francisco and Los Angeles from adopting their own privacy requirements for companies. The California legislature made clear it didn't want a patchwork of municipal level privacy laws. How is this approach any different than what Congress would be pursuing if we preempt a patchwork of State laws?

Ms. BRILL. Well, I think it certainly shows the need and the appreciation of having a uniform standard for all consumers in this market, and so I think that would be very consistent.

Senator MORAN. It interests me that already in California there is CCPA 2.0. Again, somewhat trying to combat the uncertainty different standards. But even in California, if you were preparing for a law to be enacted to take effect next year, there is at least contemplation that that law is going to be something different already. And so even within California, not only is Los Angeles and San Francisco preempted from their own, but also there may be a different statute around the corner as well. Let me do what my colleagues have done and ask all of you for a "yes or no" answer.

Understanding that there is stakeholder interest in establishing a uniform Federal framework that consumers can count on, no matter what state they live in, it is fair to say that such a framework will need substantively or at least strong policy and resource components included in order to provide meaningful privacy protection to consumers while also gaining necessary bipartisan support for possible enactment of Federal law.

Let me highlight what Senator Blumenthal says, we have bills and I am pleased that the Ranking Member and the Chairman have introduced legislation but ultimately the Senate requires 60 votes and finding that, threading that needle to find the place, is a conversation that I think we as Senators have to have, what are

we willing to accept to have something different than what we are going to have without Federal legislation.

So trying to find that bipartisan support and I would commend Senator Blumenthal for his tenacity and efforts to accomplish that goal, and I have appreciated the chance to work with him as well as Senator Wicker and Senator Cantwell and Senator Schatz and Senator Thune. That being said, do you think it would be appropriate to include the following components in a pre-emptive Federal privacy bill? Standardizing—this is the first option. Standardizing specific transparency requirements along with consumer controls and rights that will allow individuals to access, delete, or correct their personal data handled by businesses?

Ms. BRILL. Yes, that would be a critical component of any strong Federal privacy law.

Senator MORAN. Thank you.

Ms. OHLHAUSEN. Yes.

Ms. MOY. For sure, that would be included.

Senator MORAN. Thank you.

Ms. O'CONNOR. Yes.

Senator MORAN. Thank you.

Ms. RICHARDSON. Yes.

Senator MORAN. Thank you. Providing the FTC first time civil penalty authority?

Ms. BRILL. Yes.

Ms. OHLHAUSEN. Yes.

Ms. MOY. Yes.

Ms. O'CONNOR. Yes.

Ms. RICHARDSON. Yes.

Senator MORAN. Providing the FTC targeted rulemaking authority that will "future-proof" legislation without undermining the measurable certainty of the statute?

Ms. BRILL. Yes, rulemaking authority will be necessary.

Ms. OHLHAUSEN. Yes, targeted rulemaking.

Ms. MOY. With the caveat that we may define targeted differently, yes.

Ms. O'CONNOR. What she said.

Ms. RICHARDSON. Yes.

Senator MORAN. Thank you. Establishing new FTC authorizations for appropriations to address the resources and staffing needs of the agency?

Ms. BRILL. Absolutely.

Ms. OHLHAUSEN. Yes.

Senator MORAN. Ms. Ohlhausen, I would ask you to go beyond yes. Based upon your previous experience, what resources—what is the level, the nature of the change that's necessary?

Ms. OHLHAUSEN. So I do think the FTC needs substantially more resources. Its entire budget is only slightly over $300 million and that is for both missions. So I think it needs the ability to hire personnel. It needs finances, the ability to have experts, and the additional powers that a statute might provide like first time civil penalty authority, increased authority over certain entities, and the ability to create a redress fund that can repay consumers directly and promptly. I think all those are very, very important strengthening pieces for the FTC.

Senator MORAN. Thank you. Ms. Moy?
Ms. MOY. Yes, absolutely.
Ms. O'CONNOR. Yes.
Ms. RICHARDSON. Yes.
Senator MORAN. Mr. Chairman, this is my last yes or no question. Authorizing State Attorneys General to enforce the Federal standards and complement the FTC's enforcement efforts?
Ms. BRILL. Yes, that is very important.
Ms. OHLHAUSEN. Yes, and it has been something that has worked well in COPPA.
Ms. MOY. It is a critical component.
Ms. O'CONNOR. Yes, we support it.
Ms. RICHARDSON. Yes.
Senator MORAN. I would highlight, not that I am looking for the burden but I also appropriate for the FTC in addition to authorize for the FTC, and this is an important issue, I believe, for us to work out in authorization as well as in the appropriations process.
Thank you, Mr. Chairman.
The CHAIRMAN. Thank you, Senator Moran.
Senator Markey.

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

Senator MARKEY. Thank you, Mr. Chairman. Children. For all of the panelists, do you agree that a comprehensive privacy law must include heightened protection for kids and for teens, for kids in our country under the age of 16? Do you all agree that has to be much stronger than for adults? Ms. Brill?
Ms. BRILL. Yes, and I applaud all the work that you have done in this area. Absolutely.
Ms. OHLHAUSEN. Agree with heightened protections.
Ms. MOY. Yes and thank you for your leadership.
Ms. O'CONNOR. Yes, and as a mother I can say the most important thing in my household.
Ms. RICHARDSON. Yes.
Senator MARKEY. Thank you. I have introduced, you made reference to it, legislation with Senator Hawley to protect kids and teens privacy. The legislation is an update to the Children Online Privacy Protection Act, the COPPA law which I authored back in 1998. Our Markey, Hawley COPPA 2.0 bill revises COPPA's actual knowledge standard to a constructive knowledge standard so that websites that should reasonably know that kids are on the websites need to get consent in order to collect children's data.
This is a much higher standard than exist today. Ms. Moy, can you quickly explain why a constructive knowledge standard will help protect children's privacy by stopping websites from turning a blind eye to the fact that kids are on their platforms?
Ms. MOY. Absolutely, and this is really important to me. In addition to doing a lot of work on children's privacy, I have a 6-year-old who recently got his first iPad and I have been very concerned. So yes, I think that currently under the actual knowledge standard we really do have an incentive problem because that is such a high bar. Some entities that should become subject to COPPA kind of have an incentive to instead frame their sites or services is a gen-

eral audience and then look the other way about the fact that there are children on them.

A constructive knowledge standard would impose a reasonable duty of care on sites and services to know that they probably have children on their site, and it also creates an objective standard. So because the actual knowledge standard is subjective and based on what the entity actually knows, it is a little bit difficult for outsiders and enforcers and academic institutions like ourselves to actually know what those entities know and don't know.

Senator MARKEY. OK. So again, historically bad actors have targeted kids. Let us just be honest about it. It goes on today and we just need to heighten the protections. The legislation also bans targeted marketing to kids because companies shouldn't be creating profiles of eight-year-olds and bombarding them with ads. Ms. Brill, do you agree with a ban on targeting ads to kids?

Ms. BRILL. Absolutely. And Microsoft does not currently market to kids under 16. We think that that should be a rule across the Nation.

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

Ms. MOY. Absolutely.

Senator MARKEY. Do the others agree with that? Ms. Ohlhausen, do you agree with that?

Ms. OHLHAUSEN. My recollection of COPPA is that it puts it in the hands of the parents to decide if they wanted to do that. So it is something I would certainly be interested in hearing more about.

Senator MARKEY. But otherwise a ban in place. If the parents want a ban, would you support a ban?

Ms. OHLHAUSEN. Of course.

Senator MARKEY. Do you agree with that Ms. O'Connor?

Ms. O'CONNOR. Yes.

Senator MARKEY. Ms. Richardson.

Ms. RICHARDSON. Yes.

Senator MARKEY. The Federal Trade Commission recently reached a settlement with YouTube over widespread violations of COPPA. The Federal Trade Commission found that YouTube knowingly broke the law by tracking kids in order to rake in advertising dollars without the requisite notice to and permission from the parents. Ms. Moy, what did the YouTube case reveal about the corporate appetite for kids data online and the need to invest in enforcement or privacy laws?

Ms. MOY. Thank you for the question. Yes. So as anyone with kids knows, if they drive a substantial amount of household spending, this action was in response to a complaint that was filed by the clinic that I now direct. And it really did show that the children are a lucrative target and that YouTube had been widely boasting its ability to reach children, to help advertisers reach children on the one hand, and then at the same time claiming that it was not a child-directed service or did not have child-directed portions of the service.

Senator MARKEY. And again, it is like smoking or vaping. They got to get you young. They want to get you hooked young so we know that that is the business model and if we don't put in the protections, that they will try to do that. And I have called for the

creation of a youth privacy and marketing division at the Federal Trade Commission, which would be responsible for addressing the privacy of children and minors and marketing directed at children and minors in our society. It is time that we just realize it is an exploitable market that doesn't have sufficient protections.

And finally, Amazon Ring, connected to doorbells, Ring allows law enforcement to request the video footage from users doorbells, but Amazon's responses to a series of letters I sent revealed that Ring has no restrictions on law enforcement sharing users' footage with third parties and Ring has no policies that prohibit law enforcement from keeping shared video footage forever. And I was also disturbed that Amazon refused to commit that it won't sell users' biometric data that they gather.

Ms. Moy, you have testified about the importance of data use limitations in any Federal privacy bill. Should those limitations include a ban on the sale of biometric information?

Ms. MOY. You know, Senator, if your Social Security number is compromised, you can change it, but you can't change your body. And for that reason I do agree that that should be banned. There should not be a market for this information. It is too sensitive and there is no redress if it is compromised.

Senator MARKEY. I agree with you and that should be in any privacy bill. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey. Senator Blackburn is recognized, and Senator Blackburn will preside in my absence while I run, vote, and come right back.

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

Senator BLACKBURN [presiding]. Thank you, Mr. Chairman, and thank you for the Committee today and for each of you being here, and for participating in this hearing. I appreciated Senator Cantwell's remarks about it being an all-female panel and I think one of those reasons is because as I have talked with each of you over the last several years, this is a primary issue for women. They want to protect their virtual you and the virtual you of their children and protect that privacy online.

And I think people are absolutely appalled that we have gone this long without having a Federal privacy standard. It was six years ago that we started the privacy working group in the House and to think that it has taken this long to move to this direction is really surprising. But I will say I am so pleased to see so many of the components that we have discussed through the years beginning to be points that people are coalescing around, things like a Federal preemption and a Federal standard, and guarding specifically that sensitive data, and making certain that we are not focused on delivery systems anymore, which is what used to be the standard.

And I know Ms. Ohlhausen, you remember those conversations, but we are focused more on that in-use and beginning to put those protections that are in place as we look at artificial intelligence. And Ms. Moy, I appreciate your comments about that. I have got just a couple of questions I want to drill down on. Ms. Ohlhausen, I think I am going to come to you first. Let's talk about this

using—about incumbents using privacy legislation as you said as a method for raising their rivals' cost.

And as we look at keeping the Internet free and open and healthy, we talk about keeping it innovative. So as we talk about putting a privacy and data security framework and those guidelines in place, we don't want to do something that is going to embolden big tech and make competition more difficult for new entrants into the marketplace. So do you see a private right of action as a new tool that big tech could use to keep competition at bay?

Ms. OHLHAUSEN. Well, one of my concerns about a private right of action is that I think when you have a strong law, like what is being considered that gives the FTC additional resources, additional tools and empowers 50 State Attorneys General to bring these actions, that has a comprehensive and clear framework, a private right of action, I don't see how it gives consumers additional benefits——

Senator BLACKBURN. Well, and TCPA taught us that the road to protecting consumers' privacy is many times paved with good intentions——

Ms. OHLHAUSEN. Absolutely, Senator.

Senator BLACKBURN. But very difficult and fraught with peril.

Ms. Brill, any comment on that?

Ms. BRILL. We would be concerned that—we need strong enforcement. We have already talked about that. Strong Federal enforcement at the FTC, strong State Attorney General enforcement. We think that consumer redress is important, but we need to keep it targeted on what consumers actually need.

And just to be clear, you know, Microsoft has a very different business model. We are focused on ensuring that our customers succeed. Some of them are very small, some of them need to reach the market, and we are concerned with how they will navigate a world where there are multiple laws that could be difficult for them.

So in terms of though the private right of action, what we would like to see is ensuring consumers have redress where they need redress, and otherwise, we rely on Federal enforcement and State enforcement.

Senator BLACKBURN. OK. And I appreciated your comments about State level efforts. And I do think that that is an indicator of how people are saying you all need to do something about this, because they no longer have the ability to protect themselves or feel they don't have the ability to protect themselves online. The other question I have, I am going to ask you all to submit in writing on this. I think we have come to the point that we agree, there should be one regulator.

And in my opinion the FTC is the most qualified to be the regulator. They have that historic knowledge. But what I would like to see is in your perfect world, and each of you have looked at this for a long time, what should that look like? When you talk about the tools, when you talk about the ability to put those penalties in place and those enforcement and being able to address this.

This is the new marketplace and it needs to be properly staffed and then conducting itself in the proper manner. And with that I

will yield back, and Senator Baldwin, you will be recognized for 5 minutes.

Senator BALDWIN. I will yield—Senator Tester was here when the gavel——

Senator BLACKBURN. OK. Senator Tester, you are recognized five minutes.

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

Senator TESTER. Thank you very much. I want to follow up on Senator Blackburn's last point because I just want to make sure we are clear. Are you—and by the way, thank you for your testimony. Are you all in agreement that the FTC needs to be the regulator and that we only need one regulator?

Ms. BRILL. At the Federal level, yes. We agree it should be the FTC.

Ms. OHLHAUSEN. Yes, the FTC but allowing the State AGs to enforce to the Federal standard.

Ms. MOY. I would want to see how strong the standards, how strong the mandate, and what the definitions are before answering that question definitively. I will say in general, it is always good to have more cops on the beat.

Ms. O'CONNOR. We are in agreement that the FTC with the State AG.

Ms. RICHARDSON. Yes.

Senator TESTER. OK. And so the question because manpower—because I think you have all addressed the issue that they are not staffed to the point they can be. Do any of you have any idea on what the numbers might be for additional staff? And I know we have touched on a little bit, but I don't know that we actually got to numbers. Do you have any idea on what they would need in addition?

So 40 people are now working on, is that correct? They have 40 people available?

Ms. BRILL. I have heard it is 40 to 60. It is a very—it is a paltry number compared to the task.

Senator TESTER. What do you think they need?

Ms. BRILL. I would say 500.

Senator TESTER. OK. Anybody else have anything they want to throw in? Is that where we need to end up at?

Ms. OHLHAUSEN. I think going scaling up from 60 to 500 is a bit of a challenge. Somewhere in the middle and perhaps look to the FTC for the number——

Senator TESTER. So, I am looking at an ideal world not the real world. And in an ideal world, what do we need to have for people to be able to meet the needs out there in this particular area?

Ms. OHLHAUSEN. One other thing I want to mention is it is not just having people, it is also resources, right. So if they need to hire experts because often in trial you need an expert. When I was the Chairman a big part of the spending was on experts.

Senator TESTER. OK. I got you. And I mean there is no doubt about that. Manpower, resources have to come with it. And I guess it is up to us to find out where those resources come from. I assume

a self-funded agency is not part of the equation or should be part of the equation? Go ahead. You have been on this thing.

Ms. BRILL. Yes, and actually and we have seen criticism in the past decades of State Attorneys General that used resources to fund themselves. So I think that it is very wise to set up some kind of victim fund or redress fund, but I think appropriations is a better way to go.

Senator TESTER. OK, that is good.

Ms. MOY. And if I can just offer the additional—I would be remiss not to mention that many have also advocated for an independent data protection authority. You know, so when you are talking about the possibility of hiring 500 staff to work on privacy, it is at least an idea that should be considered. But again, I think that it all depends on how clear the mandate is on privacy and how strong the authority.

Senator TESTER. Yes. And so—and Senator Schatz got into this a little bit on the consent. And I know the figures were thrown out that 4 out of 5 people don't think they have any control, and 4 out of 5 people think the risk outweighs the benefits. I am surprised that it is only 4 out of 5.

I would think that it would be single percentages that actually know what their data is being used for. So the question I have, just when it comes to something basic like consent and how complicated it can be and how you really can't check out of the 21st century, how do we as policymakers make it so that those consent forms are understandable? Do we actually delineate that it has to be at a third grade level, or what do we need to do? Anybody can jump in on this by the way. Sure, go ahead. We are going to go to Ms. Richardson.

Ms. RICHARDSON. I would propose, you know, adopting the consent structure that has already been proposed by the Chairman and the Ranking Member. I think those are actually good examples.

Senator TESTER. They will function properly?

Ms. RICHARDSON. Yes, but I would say the most important thing to focus on is what is outside of notice and consent, what is so important that we just offer those people rights, regardless of what box they check, right. And that is a much harder task, but it is a worthwhile one to make sure that as people move seamlessly across devices and websites and services, that they have the same rights wherever they go.

Any time used to rehabilitate notice and consent and the hundreds of relationships we have with companies, you know, focus instead on use limitations.

Senator TESTER. This is my opinion, but I mean, I think there is very little doubt that a patchwork system doesn't work very well. And I think that we can't expect anything but a patchwork system unless we come up with a law at the Federal level. But once we come up with a law at the Federal level that empowers the states be able to do the enforcement, I think that could be the best of both worlds. That is just my opinion.

Are any of you guys lawyers? Good. We got a couple. So data that is used to harm users, that creates substantial injury. I am a farmer, OK, but is substantial injury defined within the code? Do we

know what that is? Or is that something we are going to leave the FTC to define or should we define it? Go ahead.

Ms. MOY. So, I think that the draft bill or the bill, I am sorry, would—it defines injury as including financial, physical, or reputational, right.

Senator TESTER. But to what level? I mean my reputation gets damaged every day in this job.

[Laughter.]

Ms. MOY. Right. And I think that this is one reason why it is really—so the FTC actually has a number of cases that it has enforced where it has defined some of these terms, but it has been difficult for the FTC to peg injuries that are not financial in nature to injury in the past. And I think this is one of the reasons that it is important to create the ability for the FTC to define what those injuries look like outside of financial wealth.

Ms. BRILL. You know, I will note that the——

Senator BLACKBURN. The gentleman's time has expired.

Ms. BRILL. I am sorry.

Senator TESTER. Yes, we can get on to it later. Thank you.

Senator BLACKBURN. Mr. Young.

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

Senator YOUNG. Thank you, Chairman. Since the recession, economic dynamism, business startup rates have been at least what is a modern era all time low, and as we approach, you know, the possibility of implementing somewhere here in the near term, a Federal data privacy standard, we want to make sure we don't exacerbate that trend. And something that my colleague, Senator Blackburn discussed a bit earlier about the threat of incumbents raising rivals' cost, she asked a couple of questions as it relates to the private right of action.

But I would like to broaden the scope of that question a little bit and just ask each of you to discuss particular principles or provisions, if included in a national data privacy framework, that you believe would be harmful to new firms or small firms and startups? So what protections, to put it differently, should be left out or included in this standard for small businesses or future small businesses?

Ms. BRILL. One of the things I alluded to earlier in this hearing was a concern of an overemphasis on sharing with third parties. I absolutely agree and Microsoft agrees that there should be some disclosures around that, but we need to recognize that small businesses often need to rely on third parties. They don't have within their own structures a full soup-to-nuts advertising program, just as an example, or a full slate of the kind of data that they would need to reach consumers. So if we want to ensure that small businesses have the ability to reach consumers in the same way that some of the very, very large tech firms do, we need to recognize that those companies have to rely on third parties.

And so if we overly burden the small companies through disclosures that they have to make about third parties when some of those third-party relationships are quite reasonable and would be

expected by consumers, I think we are going to put our thumb on the scale of competition.

Senator YOUNG. Are you suggesting that maybe we should have different treatment at a certain threshold, either the size of business or sales or something?

Ms. BRILL. Both bills of both frameworks do have a small business exception. They function differently. What I am also suggesting though is we should focus on what companies are doing for processing of data themselves, not only how they are dealing with sharing of data. We need to look at large companies and what they are doing internally.

Senator YOUNG. Thank you. Ms. Richardson, I think you wanted to——

Ms. RICHARDSON. Yes. I think this is something that Chairman Wicker gets right. He exempts small businesses from the more process-oriented or procedural things, but still reserves, you know, individual rights, data security, and things that are more reasonable to ask small businesses to do, so we would recommend that approach as opposed to exempting them from the law altogether because they are collecting and using the same sorts of data.

Ms. OHLHAUSEN. If you look at the FTC's 2012 privacy report, one of the things that it talks about is context and consumer expectations and permissible uses. So not requiring a lot of excess notification for things that companies just normally do and that consumers expect and that do have a high risk for consumers. So it would reduce the burden.

Senator YOUNG. So I heard earlier from Ms. Richardson this is something Chairman Wicker got right. Is there something in a separate piece of legislation or through a separate initiative we may get more right in order to ensure that small business development is neither constrained, perhaps even catalyzed?

Ms. O'CONNOR. If I could call out the portability provisions in Ranking Member Cantwell's bill. We believe that obviously data is essential to competition and we would want to see consumer rights of access and portability used to promote the consumers interest in their own data and not to create unhealthy, you know, limitations on competition. Surprisingly, even though Walmart is a big company, we are in a sector that is highly, highly competitive and we are concerned about the weaponization or the misuse of a portability concept.

Also, we are very supportive of and concerned about the legitimate uses of data such as disaster recovery or emergency operations that might not be enumerated in any of the bills, but that would be essential for small and large businesses alike.

Senator YOUNG. I may a follow up on that last point. Thank you much, Madam. I am basically out of time.

The CHAIRMAN [presiding]. Senator Rosen, you are recognized.

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

Senator ROSEN. Thank you, Chairman. Well, I have to say as a former computer programmer, I look at this panel of women and it just warms my heart, and so for all the young girls out there that I hope might consider watching C-SPAN——

[Laughter.]

Senator ROSEN. This is the hearing they should be seeing, and you are the role models that are there for them. And so I thank you for your important and hard work to get where you are and have this very important conversation because we need to have a common core of privacy protections accountability requirements because business has to operate across all 50 states, across the global market. Protecting the rights of our individuals, of ourselves, you are not only advocating for your business or for the Government, whatever it is, you are also a consumer, a person, a family member.

And so this discussion about how we talk about the work side of us, the professional, the business, the marketing and also the personal side of us and where that intersects, this is really at the core of these privacy discussions. And so I want to—I am going to submit some questions about disaster recovery. I know a little bit about that from my prior work, but today I want to talk a little bit about cyber and data security.

As Ranking Member Cantwell alluded to, data breaches have created a record pace in 2019. Over 4 billion records, 4 billion, exposed in the first half of this year alone. And for the sake of time I don't have to talk about the cost not just to industry but personally to people.

The loss of trust is also large for businesses, for individuals. Where are the trusted sources? What do we do? It is critical to all of our success. But large businesses still only spend a very small part of their IT budgets on cybersecurity, typically between 16 and 14 percent, and small businesses who face major financial consequences without the wherewithal that large businesses have, often less.

And in Nevada, although you think of us as large casinos and all those kinds of things, 99 percent of businesses in Nevada are small businesses—99 percent. And so data security for the growth of our state, our longevity, and our integrity for those small businesses that support our industry is really important.

So to everyone on the panel, what do you think the biggest impediments are to businesses taking action before the breaches happen? And as we look at it through the lens of regulation, how can we incentivize and empower the businesses large and small to take their data security seriously, protecting that consumer data thus protecting their own self-interest, I think, in the long run.

Is it through incentives, guardrails, a combination of both? What do you think we can do, because really when those breaches happen, the loss of goodwill for all of us is big. Will I shop again at that store? Will I do XYZ? Or not to mention small businesses going out of business at a large rate. Thank you. Please.

Ms. BRILL. Well, one of the things that I think is important to recognize—first of all, thank you for your question. It is an incredibly important question. One of the things that I think would be helpful to recognize is that requiring companies to provide data subject rights, to provide consumers with access to their data just as an example, or the ability to delete their data if they ask, that has an incredible effect inside a company. If you are required for each and every one of your consumers to know where that data is——

Senator ROSEN. So you think that will help against breaches, is this what you are talking about?

Ms. BRILL. What I am saying is, it creates a great deal of hygiene within a company around the data that you have. It causes companies to say, gee, there is a bunch of data I don't need. I am going to delete that data. And it really focuses a company on what is the data I need because I am going to need to provide that data to a user when they ask for it. That in and of itself is very helpful hygiene, so that if there is a breach, you are really only talking about data——

Senator ROSEN. So limiting vulnerability and exposure?

Ms. BRILL. You have greatly reduced the surface area of exposure, yes.

Ms. OHLHAUSEN. Senator, thank you for your question. I think having the kind of approach that we have seen in these proposed bills that require entities to understand and explain what kind of data they have, why do they use it, with whom do they share it, brings forward as Commissioner Brill said, it surfaces these concerns, so they have to deal with them and then make those decisions.

I think one of the other things that is really beneficial in these bills is giving the FTC this clear authority in this area to make companies understand their accountability for safeguarding the data. I think that is very, very key here. I also liked how Senator Wicker's bill looked also to the NIST framework, which is a process based. So that is also very useful even for a small business to consider.

Ms. RICHARDSON. And Senator, I would say only about half of the states right now have State level data security laws of general applicability. So including it in a Federal privacy law will cover much more people. I would say we would take what is in the Wicker and Cantwell proposals but also give the FTC general rulemaking authority for data security.

I think we know exactly what they are going to do. They are going to take their guidance that has been available for many years and write it into regulation and it is very good. It scales for different sizes and types of businesses and getting that on paper about what is expected of them will go a long way.

Senator ROSEN. Well, because the data that you all keep is the data that the hackers want. And so there is the tension.

Ms. O'CONNOR. Thank you, Senator. The efforts that large and small businesses are making to defend their systems and protect the privacy and security of their customers' data is very significant. And so we would be supportive of a particular Ranking Member Cantwell's suggestion that there be a reasonable standard and that there should be enforceability. There is no privacy without good security.

Ms. MOY. Yes, and I would agree with others that rulemaking authority in this area is critical and giving the FTC greater resources and rulemaking authority will help make the standards clearer. For businesses, I also agree that data minimization is an important component, but I think it is very clear to all of us that we need to apply data security standards to companies of all sizes because it is no consolation to a consumer that the data that was

breached about them was breached by a small company as opposed to a large one.

Senator ROSEN. Thank you.

The CHAIRMAN. Thank you very much. Thank you, Senator Rosen.

Senator Sullivan.

STATEMENT OF HON. DAN SULLIVAN,
U.S. SENATOR FROM ALASKA

Senator SULLIVAN. Thank you, Mr. Chairman, and I want to echo Senator Rosen's comments about the panel here at the outset. As a father of three daughters, I think it is very impressive and a great example. I hope my girls are watching C-SPAN, but they are probably not so——

[Laughter.]

Senator SULLIVAN. I will tell them about this hearing though, but it is impressive. So thank you for the example you are setting and really important testimony you are providing on a really important topic, but a complicated topic. And I think you see it in the competing bills and a number of ideas, so I want to thank the Chairman and the Ranking Member for holding this important hearing and working through legislation. So a couple topics I wanted to raise.

You know, we have some big companies represented here, but one of the things I always worry about when you look at major regulations or a continuing patchwork of regulations across state lines or enshrining a private right of action is that those are issues that big blue chip companies can probably handle, but we also want to be able to make sure we are doing is creating an environment where the innovation that drives our economy, particularly in this sector, continues to flourish.

And by that, I mean the ability of small businesses, startups, to create jobs, create economic dynamism, and I worry about some of the proposals here that yes, the big guys could handle it, frivolous lawsuits or patchwork, but what we really want to do is continue to create economic dynamism in this sector in a regulatory approach that keeps the incumbents in power and gives them more authority to deal with these kind of regulations or private right of action, could really stifle the next innovative American company. Can you can—I just wanted to throw that out there. I think it is a really important topic and I am not sure that the next startup, we don't even know who it is, or the next great idea, is not represented at this panel.

Ms. O'CONNOR. Senator, if I could offer an answer. Even though we are, again, one of your biggest companies in almost every state, I think every state in the Union, one of the most amazing things I have seen in my brief time at Walmart is open call. And the hallway and home office in Bentonville where little tiny one and two-person company come in and try to sell their stuff to us.

And it is just really inspiring and remarkable because it is kind of the American dream. I want to get my things on the shelves or online, and we want to work with those companies and see them flourish as well. They are our partners, our vendors, our suppliers, and a complicated standard will not help those companies thrive

and it will not help their customers either. So we very much agree that a simple clear standard that is applicable to all.

Senator SULLIVAN. And one frivolous lawsuit could crush a company like that.

Ms. BRILL. Microsoft has—we have got millions of customers and many of them are very small. We also have some of the largest customers, but we do well when our customers do well, so we are often speaking for small businesses, medium-sized businesses, legacy businesses, as well as new startups and very agile businesses. And one of the things I have said earlier, and I worry about is, when you have a brand new law that is going online in the United States for the first time affecting sectors that have never had to deal with this before, what we need to start out with is clear regulatory guidance, rules, workshops guidance.

Let the ecosystem of small businesses, medium-sized businesses understand what their responsibilities are before we throw them into court right away with large potential damages. That is going to hurt, as you just said, largely these very small businesses as well as medium-sized businesses for whom this is brand-new as well.

Senator SULLIVAN. Let me ask Ms. Brill or Ms. Ohlhausen, if we don't have a private right of action, which I am very skeptical of, what kind of improvements to FTC authority or resources would we need to make sure that as you are developing national standards, that they are enforced?

Ms. OHLHAUSEN. Thank you, Senator. I think the FTC needs more resources, both to hire staff, but also tools that it can use through the legislation such as first-time civil penalty authority for violations, the ability to get a consumer redress fund so that it can pay out redress quickly and promptly to consumers. The FTC has long asked for authority over a common carriers too. I think that could be a useful tool for the FTC. And so those are some of the kinds of both finance and authority tools the FTC should gain.

Ms. BRILL. And I agree with that list. I would add in the resources category, the FTC has wonderful people on its staff, but they need more. And they need technical expertise. They need lawyers. They need just more individuals. Earlier, I mentioned that I thought the ideal number would be 500. I think some eyebrows went up but there is a reason for it because when I look around the world, and Microsoft does have the pleasure and privilege of being able to see what is happening elsewhere in the world, most data protection authorities for much smaller companies are much better staffed than the FTC.

And when you try to do it on a per capita basis, I mean, it really gets scary when you see the really paltry resources that the FTC is able to devote to this issue. On a per capita or per company or any measure that you might want to choose, the FTC does need to scale up very quickly if a law like this gets passed. Frankly, they should do it anyway because of the urgency of dealing with these issues, but I think the resources is probably one of the most critical issues.

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

The CHAIRMAN. Who on the panel did not get to talk about the effect on innovation? I know Ms. Richardson, I would appreciate

you helping us with Senator Sullivan's question about the effect on small innovators and startups.

Ms. RICHARDSON. I would say when we speak to entities that represent small businesses, even sole proprietors and VC fund, what we always hear is that small actors need clarity. They can design to what they need to do, but they just need to know what the rules are without hiring lawyers or going through extensive tests and balancing equities. So to the extent that we do have a law that can be readable on its face and people understand what is expected of them, that is going to benefit startups.

So we would encourage Congress to go that way. And I am skeptical of safe harbors, but to the extent that we are talking about one, that might be an avenue to you know, discourage the worst behavior but give people some room to use data.

The CHAIRMAN. Thank you.

Senator Lee.

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

Senator LEE. Thank you very much, Mr. Chairman. I want to dive back into the issue that one of my colleagues raised a little while ago about the concept of consumer harm in this area. For example, one person might regard the collection of his or her data as harmful, as a harm in and of itself. Another person might find it very helpful because it might help companies help that customer, that consumer, get more quickly to where he or she wants to go.

And so it is sometimes easy to lose sight of this. There is a difference between the collection of data and the fact that some people might find that creepy, some people might find that as a form of harm in and of itself, and something like a data breach, a willful release of private data information or something like that. They are two different things. So let's start with you Commissioner Ohlhausen. I assume I can still call you that, right?

Ms. OHLHAUSEN. Yes. Thank you.

Senator LEE. How would you characterize the harm or injury that we are focusing on here or that we ought to focus on here that consumers experience through the collection or transfer of their data as opposed to the breach of their data?

Ms. OHLHAUSEN. Thank you, Senator Lee. Consumers do have different preferences and that is why it is important two fold. One, to draw the lines between sensitive and non-sensitive data carefully to capture generally how most consumers feel about whether it is sensitive or harmful or not. And then to have the appropriate opt-in or opt-out. So you would have to opt-in for collection and use of your most sensitive data and then opt-out for non-sensitive data. And I think that best reflects what consumers want, which I think is ultimately the goal of the bill, or any legislation in this area which should be reflecting consumer choices and preferences.

Senator LEE. So in that respect, should be we be focusing on an injury as opposed to a comprehensive effort to regulate data generally? Is that a better approach?

Ms. OHLHAUSEN. Well, I think in some ways it is kind of pursuing both because having a clear set of rights for consumers so that they know if something goes wrong or if they want to change

how their data is being used or collected or shared, how they would have that information and that ability to do that. So we continue to give them that control in an ongoing way.

Senator LEE. OK. Let us apply some of that logic to some of the debate that we need to have about whether to provide a private right of action. If it is difficult for us to articulate in the abstract the harm or the injury that consumers might experience in connection with data collection, shouldn't we also raise questions about whether or not a private right of action here would be able to satisfy the Article 3 judicial ability requirements in such a way that the plaintiff could establish standing?

Ms. OHLHAUSEN. I do think standing for privacy violation has been certainly a difficult legal issue. It has been one of the benefits of having Federal enforcement. For example, the COPPA law and then enforced by the State AGs. It gets around that kind of problem.

Senator LEE. It is certainly possible that the lack of defined harm or injury attached to that could cause problems, whether Article 3 problems or policy problems. It could render a subject to abuse.

Ms. OHLHAUSEN. Yes, I agree.

Senator LEE. Ms. O'Connor, I would like to turn to you next. With respect to both the CCPA and the GDPR, we have seen a fair amount of confusion with regard to compliance and some complications with regard to what data might be covered and what data might not be covered. There are many who point out that this can be a very good thing for market incumbents who have been able to get there and establish an army of compliance specialists in advance, but that it might chill startups.

There are some further consequences that could flow from this. What are some of the unintended consequences that we might face if Congress defines the concept of data in a vague or broad manner that leaves people in doubt?

Ms. O'CONNOR. Thank you so much for that, Senator. And as I said before, we are striving mightily as a company to be ready on January 1 for the California Consumer Protection Act, and it has been a very significant allocation of time and resources and human capital. And we have the wherewithal to do that. Not every company——

Senator LEE. You are a small company, right?

Ms. O'CONNOR. Right, we are a very tiny little company. No one has heard of us.

[Laughter.]

Ms. O'CONNOR. And we are absolutely trying to do the right thing, but we have issues with the California law and of the expansive definition of sale. And you are absolutely right, some lack of clarity doesn't serve business well, but it certainly doesn't serve our customers well either. And so clearly defined, clearly scoped definitions and resources and consequences are I think the right way to go.

Senator LEE. Thank you. Thank you very much. I see my time has expired. Thank you, Mr. Chairman. Thanks to each of you.

The CHAIRMAN. Thank you very much, Senator Lee.

Senator Baldwin.

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

Senator BALDWIN. Thank you, Mr. Chairman, and Ranking Member, and to all of our witnesses today. At our last hearing on data privacy, I noted that my belief that most of my constituents really don't differentiate between a company's decision to use their data or give it to others in ways they didn't expect or agree to, and a company's failure to keep their data safe and secure from third-party criminals who want to steal it.

At that same hearing, Dr. Hartzog urged us to hold companies accountable for being good stewards of users' data, meaning that they do, in his words, everything within reason to protect us from hacks and data breaches. So I am pleased to see that the proposals that are under discussion today really do tackle the issue of data security.

Ms. Richardson, I wonder if you could elaborate on how aspects of these bills might get us to the right answer on data security. And do you think they provide the framework that will make companies good data stewards? And if not, how else can we ensure companies are taking every reasonable step to keep consumers' data secure?

Ms. RICHARDSON. Thank you, Senator. Yes, we think the bills make huge strides forward and they are defining the universe of activities that companies need to take to protect data. The good news is there is much more agreement about what is good data security than there is about what is good privacy, right.

When you look at the NIST framework, the FTC, the Small Business Bureau, it is all, you know, coalescing into the same list of behaviors and it is everything from updating your systems to training your staff to deleting data you don't need anymore. So I think this is all encompassed in the bills that were looking at now. We would just encourage that there are general purpose FTC rulemakings. They would take those principles and clarify what that means for businesses of different sophistication and sizes.

Senator BALDWIN. Thank you. Ms. Moy, there are many ways in which data collection and use practices could have disproportionate impacts on vulnerable populations, as you mentioned in your testimony, including women, racial, ethnic, and religious minorities, the LGBTQ community, people with disabilities, older individuals, and others.

I believe that both data use restrictions and affirmative civil rights protections can help mitigate these potential negative impacts, and I am pleased that the ranking member's proposal and a number of other bills by others on and off the Committee include these types of measures. Could you discuss how the proposals before the Committee speak to protecting vulnerable populations? Do they go far enough, and are there other ways we should seek to prevent discrimination in a data privacy measure?

Ms. MOY. Thank you so much for the question. This is really—I think that this is a really important issue as I highlighted in my remarks. So, just to give a few examples, information about consumers has been used not only to target advertisements for things like housing, employment, and credit in discriminatory ways, but

also to target political misinformation and disinformation at certain classes of people.

Also to target voter suppression efforts at certain classes of people. There is a lot that is potentially harmful. I think that in particular the bill that the Ranking Member has introduced in addition to outright prohibiting use of personal information for discrimination, which is key, also would force companies to take steps to determine whether or not discrimination is likely to occur on the on their platform based on their use of data.

I think that is really important because I think that without a provision like that, that requires that type of assessment to take place in advance, at times there may be an incentive, an unfortunate incentive, for companies not to develop the knowledge that discrimination is taking place on their platform so as to avoid incurring liability for that discrimination. And so I think forcing prospective awareness of it is really critical.

Senator BALDWIN. Thank you.

The CHAIRMAN. Thank you, Senator Baldwin. Senator Cantwell has some follow-up questions.

Senator CANTWELL. Thank you, Mr. Chairman. I know our second vote, I think, did just start, so I will try to be quick and if the witnesses could help me. Another kind of yes, no answer on the first part. And that is, you know, as we are talking about what is sensitive data and information, is facial recognition sensitive? Yes, if you can just yes.

Ms. BRILL. Yes.

Ms. OHLHAUSEN. I don't think the Coalition has a position on that. Yes.

Ms. MOY. Yes.

Ms. RICHARDSON. Yes.

Senator CANTWELL. That was a yes, Ms. O'Connor?

Ms. O'CONNOR. Yes.

Senator CANTWELL. OK, thank you. OK, then on, you know, one of the things we have tried to do is clarity. Obviously because predictability is an important thing. Where do you think it leads the colleagues that I have joined with in putting out a draft? Where do you think that stands as it relates to GDPR and in comparison? How do you view that as far as you know clarity? Obviously, if it was enforced the way it was enforced or what have you?

Ms. BRILL. One of the issues that I look forward to working with you and the Chairman on is ensuring that the provisions that you have put in place do not unintentionally favor some parties over other parties. I think there is a bit of a thumb, unintentional, on the scale in terms of favoring very large firms that are soup to nuts, can just surface ads to users without having to share with third parties. Again, unintentionally so——

Senator CANTWELL. That is the same problem with California today.

Ms. BRILL. Absolutely.

Senator CANTWELL. Very big problem. Listen, we are not even to have a free media in this country if we continue to persist in not clarifying those and we won't even control any of our content that we see because they will have all the money and they will plan all the content and then they will have all the advertising.

Ms. BRILL. I think that is an issue with the California law as well. I agree.

Senator CANTWELL. Yes, so we don't want that, but related to GDPR.

Ms. BRILL. Your proposal as well as the Chairman's proposal have embraced a great many of the concepts in GDPR that I think are going to be helpful for users and in particular what is very encouraging to see is that both proposals, both yours and the Chairman's, focus on user control and the real kind of data subject rights that you see in GDPR subject to the absence of a right to object to first-party processing. That is the piece that would help with this competition issue. And you also have some of the accountability measures like data minimization. Very important to require accountability on the part of companies as well. And we see that in GDPR too.

Ms. OHLHAUSEN. Yes, I think that both proposed bills provide more clarity. I think there is some ambiguity in GDPR, and I also think it less onerous as my colleague Julie Brill pointed out, on small and medium businesses.

Ms. MOY. Yes, and I agree that I think that the adopting the rights framework is a really important thing that both frameworks do similar to some of the rights that are expressed in GDPR.

And then I would also just mention that in terms of clarity, again the rulemaking authority is really critical there so that if there are issues that cannot be encoded in the statute at this moment in time because doing so might make the law less flexible to accommodate changing technology in the future, that an agency could do so in the future.

Senator CANTWELL. Ms. O'Connor.

Ms. O'CONNOR. There are many companies that have quibbles with GDPR but the one thing you can say about it is it is done, and it applies to everyone in Europe. And so——

Senator CANTWELL. Do you prefer that over what we have been talking about this morning?

Ms. O'CONNOR. No, no. That is not at all my point. Simply that a Federal standard is where we want to go because it will provide certainty for all consumers.

Ms. RICHARDSON. And I think your bill is definitely clearer than GDPR. I would say areas that I think might be subject either to litigation or exploitation in the future or anywhere that a bill references like a reasonable user, if we do not have guidance about what Congress thinks the reasonable user is, I see that being a problem where if it is, you know, substantial harm that isn't defined. So to the extent we can get even deeper on some of those issues, I think that will provide better protection for consumers and predictability.

Senator CANTWELL. Yes, I was looking at a much broader thing, but this is very helpful. So thank you. So do you think that is a better approach than GDPR or no?

Ms. RICHARDSON. Yes. For the U.S., absolutely.

Senator CANTWELL. OK. That is the main thing, and yes, that is the whole point. The more clear we can be, the more predictability we can have here. But yes, it means having definitions and it means having real enforcement and yes, a lot of these things. I

have enjoyed this discussion because we are very involved in putting anti-manipulation standards into both the FERC and the CFTC and the FTC.

And you know, a lot of people are like, no, you can't do it, you can't define manipulation. Well, I guarantee it we have collected hundreds of millions in fines against companies that have manipulated starting within Enron, electricity markets, and now other energy markets. And people have called it, you know, started out as a little acorn and has turned into a mighty oak because people knew what manipulation was. And so hopefully they will understand what harm is too and so I appreciate that everybody has supported harm today. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cantwell. I want to drill down on broad APA rulemaking authority versus targeted rulemaking authority. And you are probably aware that the current Chairman of the FCC testified before the House Energy and Commerce Committee recently, and when asked if Congress should give the FTC broad APA rulemaking authority? He answered, "please do not do it, do not give us broad rulemaking authority. Give us targeted rulemaking authority."

So help us understand this and help the public understand our choice in this regard. And I guess we will just start down here and whoever would like to participate in this question.

Ms. BRILL. Thank you so much for the question. I understood the Chairman's comments to mean don't sweep the FTC into general APA rulemaking authority, but rather allow the FTC to write rules when a specific law is enacted. I would—I interpreted Chairman Simon's remarks to indicate that with respect to a law like COPPA or with respect to a law like the ones that we are currently discussing, the bills and the frameworks, that he would probably appreciate, and maybe I shouldn't continue to speak for him.

I would say as a former FTC Commissioner, I would have appreciated having rulemaking authority for the entire bill, not for specific sections because there is so much in this bill that I think could benefit from some form of rulemaking or guidance from the FTC. Just thinking about some of the provisions you have included, data brokers as one of many examples. It is a great provision.

I applaud you for including that in your framework. Very important to provide visibility of about those entities that are operating behind the scenes that have no user interface for consumers. So you have done a wonderful job by surfacing that issue, but it is going to require some rulemaking in order to understand who is a data broker and who isn't a data broker. We have seen that in Vermont. We will see that in California, which has also adopted this law. So when I think about targeted rulemaking, there is a number of different ways to think about it.

There is just general APA rulemaking that the agency would have for everything, APA rulemaking authority for a specific law, or APA rulemaking authority for specific provisions within a law. I like the middle road that I have just described. I like—I think for this bill there is so much in it that we ought to give the FTC the ability to write rules where it sees confusion, or they need greater clarity.

The CHAIRMAN. Ms. Ohlhausen, help us understand the distinction.

Ms. OHLHAUSEN. Yes, I think the distinction and having talked to Chairman Simon about this generally, when you look at the way COPPA has worked, where Congress set out some very clear guideposts. It set the age, it said parents are going to be in control. It made a lot of the hard choices and hard definitions and then gave the FTC the job of filling in the details and keeping up with technology, such as changing what personal identifiable information maybe down the road as new technologies come onboard.

I think that is the idea of targeted rulemaking. So Congress has set the provision on data portability. It is not a requirement that the FTC just has to come up with, that there should be data portability. You are saying Congress has decided there should be data portability but then the FTC should give some content to where Congress has said these kinds of rights should be available.

The CHAIRMAN. Ms. Moy.

Ms. MOY. Yes. So I agree. I think that would be helpful to give the FTC rulemaking authority to flesh out all parts of the framework and not just one limited function. And I think, you know, if you look at, there is a couple of few things that I would give as examples. One is, definitions may need to be updated at times to account for changing technology. And so Commissioner Ohlhausen just mentioned COPPA a moment ago. For example, when the Commission updated the COPPA rule in 2013, it recognized that between 1998 and 2013, it had become clear that the face of a child could be used to identify them and contact them, and so could a voice.

And those were things that we didn't know or didn't see coming quite with clarity in 1998. So it was really important to task the agency with updating that in order to future-proof the law. And so yes, as Commissioner Brill mentioned a moment ago, data brokers as well and just providing data security, of course, but providing some functional definitions in the statute and then enabling the agency to flush them out and update them over time is really important.

The CHAIRMAN. Ms. O'Connor.

Ms. O'CONNOR. Mr. Chairman, thank you for that question, because it gives me the opportunity to applaud you and your staff's work and the provisions in your draft on targeted rulemaking and we are comfortable and supportive of those.

The CHAIRMAN. Ms. Richardson.

Ms. RICHARDSON. Yes, we would prefer that Congress make the primary policy decisions here, right. And I think that is going to come out with the best solution for users, and where the rulemaking is most useful, we think it should be targeted and not for the entire bill necessarily. If things were either, there is a lack of clarity, right, so something that is reasonableness or things are going to scale to different types of businesses or where you think technology might change over time. And those are two areas that would be most useful.

The CHAIRMAN. Thank you very much.

Senator Gardner.

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

Senator GARDNER [presiding]. Thank you, Mr. Chairman. Thank you Ranking Member Cantwell as well for this hearing today. It is a very important hearing. Thanks to all the witnesses for your time and testimony today. In Colorado, obviously, we cherish our personal privacy. It is the core of our Rocky Mountain values. It is who we are. It is our businesses. It is our own businesses unless we say otherwise. That is why I have strongly supported efforts to enact a national bipartisan privacy policy that respects Colorado's values, respects American values, consumer choice and the appropriate safeguarding of our private lives.

Ms. O'Connor, one of the most important principles of privacy is adherence to transparency for consumers. That is what led me to introduce Protecting Privacy In Our Homes Act, which would require the manufacturers of Internet of Things, IoT, devices disclose to consumers what that device, when that device contains sensitive technologies like a camera or a microphone.

A report surfaced earlier this year that the Google Nest, for example, a product that Walmart carries, contained microphones not previously disclosed to consumers and I think consumers should know what they are buying. They may want one with a microphone. They may not.

Walmart is the world's largest retailer, serves hundreds of millions of customers every week around the globe, hundred locations in Colorado, sells millions of these kinds of products and devices across a wide array of categories. Does Walmart believe that consumers should know whether they are purchasing items that contain sensitive technologies like a microphone or a camera?

Ms. O'CONNOR. Senator, thank you so much for that question. Absolutely. We agree with the intent and the construct of the bill. My only challenge would be we would like it to have a more comprehensive omnibus approach to privacy than just a product specific one, but we absolutely look forward to working with you and your office on the details of that bill and on the protections for IoT, which as you point out, we do sell we do not manufacture currently, but we very much appreciate the intent.

Senator GARDNER. And thank you because I think there was an article just last couple of week about Alexa being placed in all kinds of different devices. And so this is an important conversation that we have with the American consumer and manufacturers. Ms. Brill, I just wanted to comment on or ask a question based on something you said in your opening statement, and perhaps I get a yes or no from everybody on the panel.

In your statement, you said that "at Microsoft we believe that privacy is a fundamental human right." Does anybody on the panel disagree? OK, everybody on the panel is in agreement with that statement. You also said, I believe you said this in your statement, "consumers have a right to control their own data." Is that similar to what you said or something you said?

Ms. BRILL. Yes. Yes. I don't remember if it is an exact quote, but we absolutely believe consumers do have a right to control their data.

Senator GARDNER. And everybody on the panel agrees with that? OK. In your statement, you said unlike Europeans or Brazilians or Chinese nationals, Americans today do not enjoy comprehensive privacy protections that apply across the country. What do you mean by Chinese nationals and their privacy protections?

Ms. BRILL. Interestingly, in China there is a baseline privacy legislation. So leaving aside government surveillance, leaving aside some very big issues——

Senator GARDNER. Which seem to go to the core of privacy.

Ms. BRILL. There is no question. But what we are seeing in China is that there is a GDPR like law——

Senator GARDNER. But there can be no equivalency to U.S. privacy and China?

Ms. BRILL. Absolutely not.

Senator GARDNER. So let me get further into this then because I am going to run out of time and you have been here a long time, and I apologize for that. This right to control our own data, does it include our facial features for facial recognition?

Ms. BRILL. From Microsoft's perspective, we have called for legislation specifically focused on facial recognition technologies, including giving users the ability to consent.

Senator GARDNER. Right. So we would have that consent. So that would be handled just like the search on the Internet or something like that, that somebody would have under that kind of control, or a credit score, those kinds of things. Is that correct?

Ms. BRILL. We——

Senator GARDNER. There is a lot of nuances in there. I understand.

Ms. BRILL. There is a lot of nuances in what you just said. We do believe that users should have transparency around the use of facial recognition technology, and they should in appropriate circumstances, be able to consent to the use of that technology.

Senator GARDNER. But that consent is obviously not given in China.

Ms. BRILL. There are many issues with respect to what China is doing with a number of technologies.

Senator GARDNER. And facial recognition technology is obviously going to be used for very bad and nefarious purposes in China as they single out Uyghurs ethnic minorities, as they scan Hong Kong protesters, and decide who has a social credit score that is acceptable to travel into China, or who is going to be allowed to participate in basic freedoms that we adhere to. So I know Microsoft is working in China and has some announcements on this.

So, how do you weigh the belief that privacy is a fundamental human right, that consumers have a right to control their own data with what China is doing with facial recognition?

Ms. BRILL. So, thank you for the question. It is a very important question. Doing business in China has always been challenging, not just in the current state, but has been for a long time. We are guided by our commitment to human rights and our commitment to democratic values. When we engage with anyone in China with respect to any of our products and services, we take a very close look at not only the actual product and services involved but what are the use cases that are likely to arise, and we will refuse to provide

technology not just in China, but in other circumstances around the world where there are human rights concerns.

We take that our responsibility and our obligation to ensure that human rights are protected, including in a facial recognition circumstance. We take that obligation and responsibility very seriously.

Senator GARDNER. But is Microsoft continuing its work with China on facial recognition technologies?

Ms. BRILL. I would be very happy to get back to you with regard to specifically what, if anything, we are doing with respect to facial recognition in China. I am not aware of our doing any work on facial recognition in China at the moment, but I would like to ensure that the answer I am giving you is correct.

Senator GARDNER. And to be clear, this is broader than Microsoft. To be clear, this is broader than——

Ms. BRILL. OK, but your question was about Microsoft and——

Senator GARDNER. No, but it is also, I just want to make sure that I am not just picking and singling out you, that there are other concerns and companies doing the same thing, and it is broader than just facial recognition software. It is other technologies that could be used to breach the privacy. As everyone on the panel has said, we believe this is a basic human right and we believe that consumers should have control of their own data. That we are empowering very evil actions to take place with the imprisonment of over one million Uyghurs in Xinjiang province in Western China, and we as a country have to make sure that our values don't end where our borders end. That wherever we are doing business, our values continue.

Ms. BRILL. Absolutely. And Microsoft takes that responsibility very seriously. When I talked about our focus on ensuring that the use of this very powerful technology will be respectful of human rights, that is a Microsoft approach. I can't speak for the entire industry, but we take that responsibility and obligation very seriously.

Senator GARDNER. Thank you. Thank you for your time and to all of your testimony today. And I am going to close out the hearing here. So just appreciate—please accept the Committee's appreciation for your time and testimony today and for the questions that you have answered.

The hearing record will remain open for two weeks. This is your homework assignment. Hope that you will—Senators are asked to submit any questions for the record. Upon receipt, witnesses are kindly asked to return their answers to the Committee as soon as possible by no later than Wednesday, December 18, by the close of business. They will be included as part of the record.

So I would just like to thank you again, and this hearing is adjourned.

[Whereupon, at 12:31 p.m., the hearing was adjourned.]

A P P E N D I X

Response to Written Question Submitted by Hon. Shelley Moore Capito to Hon. Julie Brill

Question. In your testimony, you mention that Microsoft offers privacy controls to its users. West Virginia has an aging population that is at risk of falling victim to online scams and may also have trouble understanding the fine print associated with privacy controls or privacy policies. How do your users learn about those controls and how to use them effectively?

Answer. We seek to empower our consumers by providing them with transparent and easy-to-use privacy controls. Our products and services offer a number of controls and resources to enable our consumers to configure the level of privacy appropriate for them. To make exercising these controls across Microsoft easier for all of our consumers, including our older consumers, we have created a Privacy Dashboard, where our consumers can view, download and clear personal data tied to their Microsoft account including browse history, search history, precise location data, and more. Our consumers can also manage apps and services that have permission to access certain data connected to their Microsoft account, choose whether to see interest-based advertising, and update communications preferences. Detailed guidance on how to configure controls in our products and services, as well as how to set communications and advertising preferences, is available on privacy.microsoft.com.

We are very proud of our Privacy Dashboard and the privacy controls that we offer globally, including to our U.S. consumers. We believe that offering such controls is essential for protecting privacy and building trust. However, we also recognize that user controls are not by themselves sufficient for ensuring privacy protection. While more than 28 million consumers have exercised our privacy controls, we understand that many more of our consumers live busy, complicated lives and do not have the time and/or inclination to navigate such controls. This is why we have implemented a robust privacy program to ensure that we design our online services responsibly and act as good stewards of our consumers' personal information regardless of whether consumers exercise our privacy controls.

Companies, rather than consumers, should bear the primary burden of privacy protection. We encourage Congress to pass a privacy law mandating that all companies bear this responsibility, including, as has been proposed in both Senate Commerce Committee drafts, through affirmative obligations for companies to minimize the amount of personal information they collect and to conduct and document data protection impact assessments that may be subject to regulatory scrutiny. Additionally, we think that companies should be required to uphold duties to reasonably secure personal information from unauthorized access and to guard against unlawful discrimination in violation of U.S. laws.

Response to Written Questions Submitted by Hon. Amy Klobuchar to Hon. Julie Brill

According to a recent study, 81 percent of U.S. consumers feel that they have little to no control over how their personal data is used. Both my bill with Senator Kennedy and the bill that I have put forward with Senators Cantwell, Schatz, and Markey include a provision to ensure that consumers have the right to access and control how their personal data is used.

Question 1. Do you believe that consumers should have the right to access and control how their personal data is used?

Answer. Yes, we believe that enabling consumers to exercise rights to access and control how their personal data is used is essential for protecting privacy and building trust. However, we also recognize that user controls are not by themselves sufficient for ensuring privacy protection. While more than 28 million consumers have exercised our privacy controls, we understand that many more of our consumers live

busy, complicated lives and do not have the time and/or inclination to navigate such controls. This is why we have implemented a robust privacy program to ensure that we design our online services responsibly and act as good stewards of our consumers' personal information regardless of whether they exercise our privacy controls.

Question 2. In your view, what more should companies do to inform consumers about how they are using, and often profiting from, their data?

Answer. Consumers should have the right to be informed, in a concise and understandable manner, about what personal information companies collect about them, and how that information is used and shared, particularly with respect to how the data is used to generate profit. Companies should be required to provide this information in a context-appropriate manner at the most meaningful times during the experience with the consumer.

In addition to promoting transparency and consumer control, privacy laws should mandate corporate responsibility. Companies, rather than consumers, should bear the primary burden of privacy protection. We encourage Congress to pass a privacy law mandating that all companies bear this responsibility, including, as has been proposed in both Senate Commerce Committee drafts, through affirmative obligations for companies to minimize the amount of personal information they collect and to conduct and document data protection impact assessments that may be subject to regulatory scrutiny. Additionally, we think that companies should be required to uphold duties to reasonably secure personal information from unauthorized access and to guard against discrimination in violation of U.S. laws.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO HON. JULIE BRILL

Enforcement is a critical component of any data privacy law, and State Attorneys General must play an important role ensuring that these laws are followed and consumers' privacy is protected.

Question 1. Should State Attorneys General have the ability to fully enforce a hypothetical Federal privacy law? And should State Attorneys General have the ability to enforce state privacy laws—as long as they are not in direct conflict with the Federal law?

Answer. Yes, we believe that a strong Federal privacy law should empower the State Attorneys General to enforce the provisions of the law. First and foremost, Congress should empower a strong central Federal regulator, such as the FTC, to serve as the primary enforcer of the Federal privacy law, and should provide that regulator with sufficient authority, technical capability, and funding to issue rules and appropriately enforce the law. However, understanding the breadth of privacy issues needing to be addressed and Federal resourcing constraints, we believe that the State Attorneys General must also be empowered to enforce the law. State Attorneys General should also continue to have the ability to enforce state privacy laws that are not preempted by the Federal law, should the Federal law be preemptive.

Ms. Brill, you know the importance of a Federal Trade Commission that is adequately staffed and supported. I worked with my friend Senator Moran in the appropriations process to request an assessment and a report on the agency's efforts on data privacy and security as well as a needs assessment for the agency.

Question 2. Do you think the FTC is currently staffed with a sufficient number of technologists and lawyers to provide adequate oversight of companies and their privacy practices?

Answer. No, the current staffing of 40 employees focused on privacy at the FTC is not sufficient to provide adequate oversight of companies and their privacy practices. As I stated that the hearing, I think that the FTC needs about 500 additional people to accomplish the tremendous task at hand of regulating privacy in the digital age. We are dealing with an unprecedented amount of data, and we need investments in the area of data protection and privacy to not only match today's activity, but to be best prepared for this ongoing digital transformation. The FTC needs both people, including technologists and lawyers, and resources.

The disparity between the resources of the EU data protection authorities and the FTC is tremendous. Italy is a country that is one-fifth the population size of the U.S., yet Italy has three times more employees dedicated to regulating privacy than the U.S. France, the United Kingdom, and Spain all also have more regulators dedicated to the issue. The most well-staffed European privacy regulator, the Irish Data Protection Commission, has one employee working in data privacy for every 28,000 persons in that country. By comparison, using the U.S. Census population figure of

330 million people, having 40 FTC employees working on privacy means that there is just one relevant FTC employee for every 8.25 million Americans.

To further illustrate the disparity in regulatory resources, this chart lists the ratios between the number of privacy regulator employees and the number of citizens in several prominent countries:

Country	Privacy Regulator	Employees Working on Privacy	Population	Ratio
Ireland	IDPC (Irish Data Protection Commission)	180	5,068,000	1:28,000
UK	ICO (Information Commissioner's Office)	700	65,105,246	1:93,000
Spain	Spanish Data Protection Agency (Agencia Española de Protección de Datos)	180	49,331,076	1:274,000
France	CNIL (Commission nationale de l'informatique et des libertés)	195	67,364,357	1:345,000
Italy	Italian Data Protection Authority (Garante per la protezione dei dati personali)	125	62,246,674	1:498,000
U.S.	FTC (Federal Trade Commission)	40	330,000,000	1:8,250,000

A major expansion of resources dedicated to privacy is necessary for the FTC to be an effective overseer of a comprehensive Federal privacy law.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. SHELLEY MOORE CAPITO TO HON. MAUREEN OHLHAUSEN

Question. California recently released a study that indicated CCPA compliance could cost companies a total of $55 billion. In the report, California acknowledges that, "small businesses are likely to face a disproportionately higher share of compliance costs relative to larger enterprise businesses." How can we maintain a healthy environment for startups and new business development with these barriers to entry? Can you speak to how a patchwork of state laws will impact small businesses and startups?

Answer. As you reference in your question, the State of California has recognized that startups and small businesses that fall under the CCPA are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.[1] Similarly, the European Union's General Data Protection Regime has harmed small businesses, which lack the resources of large corporations to develop compliance regimes for highly complicated laws. In addition, a patchwork of different, and potentially conflicting, state privacy laws exacerbates the challenges of complying with one complicated regime by requiring small entities with limited resources to examine and adapt to requirements on a state-by-state basis.

Spending money and time complying with complicated legal requirements deprives small entities of resources they could otherwise devote to developing new products and services and entering new markets. This dynamic creates barriers to entry for start-ups. Congress can avoid creating such barriers to entry by enacting Federal privacy legislation that includes strong, but clear, consumer protections that are not over complicated and that alleviates the challenge of differing state privacy laws by replacing them with a single, national framework. With a national and uniform set of protections and consumer rights, startups and small businesses would no longer be at a competitive disadvantage relative to larger enterprises, who can spend more to maneuver through complex regulatory regimes and adapt more readily to each new state law or amendment that emerges.

The proliferation of state privacy laws creates significant compliance and operational challenges for startups and small businesses. State privacy laws are constantly being enacted and existing laws are rapidly evolving. Each law requires

[1] *http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf*

qualifying businesses to take compliance actions that go beyond standard business practices, implement new systems to respond data related requests, and be subject to unique fines and penalties. And, unlike larger enterprises, startups and small businesses are less likely to have significant in-house regulatory resources that would allow them to quickly adjust to this evolving patchwork of state laws.

Most startups and small business are generally ill equipped to absorb the large up-front costs to comply with each state law or maintain compliance in the face of uncertainty in the future that emanates from over complex or ambiguous laws. Initially, startups and small businesses incur large legal fees while preparing for and interpreting each new law. Legal counsel is necessary for businesses to have compliant privacy policies, and so that internal operational and technical plans can be made. Next, startups and small businesses may have substantial operational and technological costs as they may need multiple departments to coordinate on the compliance strategy and workflow. Startups and small businesses will likely have to redesign their websites, edit forms, and establish technologies to respond to consumer requests and other aspects of state laws. Lastly, business decisions may change as state laws are adopted and amended, including renegotiating contracts with service providers and amending business plans to change the way personal information is handled or sold. But startups and small businesses may not have the negotiating power to push back on service provider contracts or the capacity to change business models to accommodate the multitude of differing state requirements.

Thank you again for the opportunity to respond to your post-hearing question and testify at the hearing. The Coalition looks forward to working with the committee and all stakeholders to craft strong, national privacy legislation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO HON. MAUREEN OHLHAUSEN

Enforcement is a critical component of any data privacy law, and State Attorneys General must play an important role ensuring that these laws are followed and consumers' privacy is protected.

Question 1. Should State Attorneys General have the ability to fully enforce a hypothetical Federal privacy law? And should State Attorneys General have the ability to enforce state privacy laws—as long as they are not in direct conflict with the Federal law?

Answer. Allowing State Attorneys General (AGs) to enforce a Federal privacy law would give consumers greater protection while still maintaining a uniform set of protections and consumer rights throughout our digital economy. The FTC has limited resources and allowing State AGs to enforce a Federal privacy law would supplement the FTC's enforcement power. It would also permit State AGs to focus on violations affecting the citizens of their state. A Federal privacy law that permits AG enforcement would remedy the problems created by a patchwork of data privacy laws while leveraging the existing State AG enforcement infrastructure to provide greater protections for consumers. This model has worked well for the Children's Online Privacy Protection Act, for example.

A Federal privacy law should provide a national and uniform set of protections that State Attorneys General could enforce. The goal of a uniform system—clarity and certainty for consumers and business—would be lost if State AGs were simultaneously enforcing differing State laws. A proliferation of different State privacy requirements creates inconsistent protections for consumers, as well as significant compliance and operational challenges for businesses of all sizes. I am concerned that having a provision in Federal legislation that states can continue to enforce state laws that do not directly conflict with a new Federal law would result in uncertainty and litigation regarding whether a state law directly conflicts with the new Federal law. Instead, the FTC and State Attorneys General should unite to enforce a uniform Federal law.

Thank you again for the opportunity to respond to your post-hearing question and testify at the hearing. The Coalition looks forward to working with the committee and all stakeholders to craft strong, national privacy legislation.

Question 2. Ms. Ohlhausen, you know the importance of a Federal Trade Commission that is adequately staffed and supported. I worked with my friend Senator Moran in the appropriations process to request an assessment and a report on the agency's efforts on data privacy and security as well as a needs assessment for the agency.

Do you think the FTC is currently staffed with a sufficient number of technologists and lawyers to provide adequate oversight of companies and their privacy practices?

Answer. As our economy and the collection, use, and sharing of personal data has continued to grow, the FTC is reaching the limit of its current tools and resources, including personnel such as lawyers and technologists. As it stands, the FTC has an annual budget of approximately $300 million and employs approximately 1,100 staffers to carry out its consumer protection and competition missions.[1] Despite the growing need for privacy enforcement, the FTC's budget has been flat since 2013 and the number of full-time employees lags behind where it was in the early 1980s. The annual budget and number of staffers is already lean, and the agency will need additional resources to handle the work of enforcing of a Federal privacy law, as well as several related rulemakings required by the proposed legislation. Allowing the State Attorneys General to enforce a new Federal law will help, but expanded resources for the FTC is also essential to enforce a new comprehensive Federal privacy law.

Thank you again for the opportunity to respond to your post-hearing question and testify at the hearing. The Coalition looks forward to working with the committee and all stakeholders to craft strong, national privacy legislation.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO LAURA MOY

In October, the *Washington Post* reported that at least 44 universities in the U.S. are tracking prospective students on their websites and collecting information—which can include data on their web-browsing habits, ethnicities, household incomes, and test scores—to help them determine which students to admit. Many of these universities do not allow students to opt out of data collection or even tell students they are collecting this information. My bill with Senators Cantwell, Schatz, and Markey includes a provision to allow consumers to opt out of the collection and sharing of certain data.

Question. Should consumers be able to opt out of having certain data collected and shared, and can you speak to the implications of this type of data being made available to companies without consumers' knowledge?

Answer. Yes, consumers should have a choice about whether their information is collected and shared. Information about students' browsing habits, ethnicities, household incomes, and test scores likely will reveal highly private details about their lives. For example, browsing history can be used to infer a person's political, romantic, and sexual preferences—details that many individuals would choose not to share if they were given the choice.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO LAURA MOY

Enforcement is a critical component of any data privacy law, and State Attorneys General must play an important role ensuring that these laws are followed and consumers' privacy is protected.

Question 1. Should State Attorneys General have the ability to fully enforce a hypothetical Federal privacy law? And should State Attorneys General have the ability to enforce state privacy laws—as long as they are not in direct conflict with the Federal law?

Answer. Yes, State Attorneys General should have the ability to fully enforce any new Federal privacy law as well as state privacy laws. The fact that a majority of Americans describe the current lack of privacy protections as a "crisis" indicates that we don't just need additional legal protections; we also need far more cops on the beat.

It is clear that some data can be very harmful to consumers if it is not handled safely and securely, if it has to be collected at all. Biometric data systems such as facial recognition can be overly invasive and, if misused, can cause housing or job discrimination. Children are too often preyed upon online. Data compiled from different sources can be used to build profiles of individuals and skirt privacy laws. And the capabilities to collect and manipulate data with artificial intelligence will only advance as time goes on.

---

[1] *https://www.ftc.gov/system/files/documents/reports/fy-2020-congressional-budget-justification/fy_2020_cbj.pdf*

Question 2. Ms. Moy, when looking at the several data privacy bills put before our committee, do you believe current definitions of "sensitive data" are sufficient to cover our most private information? Are the proposals being discussed here today enough to protect highly sensitive personal data now, and also in the future?

Answer. I am pleased to see that there are multiple bills before the committee that define sensitive data in a way that encompasses important categories of information such as biometric data and health information. There are, however, important differences among the bills, and I highlight a few in particular. First, communications metadata should be considered sensitive. Without even looking at the contents of a person's communications, one can learn many details about a person's private life just from metadata disclosing the parties with whom the person communicates, the amount, the times, and the frequency. Metadata alone can reveal information about a person's closest relationships, financial and health providers and activities, political activities, and more.

Second, information that reveals online activities over time and across sites or services should be considered sensitive. This information may also be considered metadata regarding online communications. Regardless of what category they fall into, web browsing and app usage histories should be protected as sensitive information. The apps and websites a person uses and visits frequently reveal details about romantic interests, sexual activities, health activities, and the operation of devices and services—such as baby monitors and connected appliances—within the home.

Third, medical data should be considered sensitive. This should extend not only to information about a person's diagnosis and treatment collected and maintained by healthcare providers, but also to information about health that is collected and maintained by third parties, as well as to non-health-related information that is used to draw inferences about a person's health. For example, consider the fact that a savvy party with access to data generated by motion sensors on a mobile phone can draw inferences about whether or not the phone's owner has Parkinson's disease from that data. Protections for sensitive information should extend to the underlying data at the time that it is collected or processed for the purpose of determining whether or not the data subject has Parkinson's or any other health condition.

Fourth, nude or intimate photos and videos of people should be considered sensitive. These types of information should not be collected, processed, or shared without the explicit opt-in consent of the data subject.

Question 3. Your testimony highlighted the efforts by state legislatures to step into the void caused by the lack of a Federal law. There is a criticism that it is too unmanageable for corporations to comply with different state laws as well as international laws governing data privacy and usage. But the point of a privacy bill should be to protect consumers—not protect companies from state laws. Is it possible to find a balance that preserves a strong role for states in a Federal privacy law that also provides more certainty for business than they have today?

Answer. I do believe it is possible for a Federal privacy law to provide more certainty for businesses, while also preserving a strong role for states. As this question notes, states are currently very active on privacy in large part because there *is* a "void caused by the lack of a Federal law." If a strong Federal law were to pass, even if it did not prevent states from passing their own, stronger laws, it would slow or even stop the current trend at the state level, because many state consumers and legislatures would be satisfied that privacy needs had been met by passage of the strong Federal law. A strong Federal law should set a floor, not a ceiling, for states.

Response to Written Questions Submitted by Hon. Shelley Moore Capito to Nuala O'Connor

Question 1. California recently released a study that indicated CCPA compliance could cost companies a total of $55 billion. In the report, California acknowledges that, "small businesses are likely to face a disproportionately higher share of compliance costs relative to larger enterprise businesses." How can we maintain a healthy environment for startups and new business development with these barriers to entry? Can you speak to how a patchwork of state laws will impact small businesses and startups?

Answer. Even though we are one of the biggest companies in almost every state, many of our partners, vendors, and suppliers are small businesses and/or startups. A patchwork of state laws will not help these companies thrive and it will not help their customers either. The solution is a simple, clear Federal standard that is applicable to all.

Question 2. In your testimony, you note that Walmart uses data to manage their supply chain and efficiently fill and ship orders. West Virginia is home to a brand

new Proctor and Gamble facility that I imagine is one of those suppliers, but I am sure many of your suppliers are also small businesses. How would CCPA and the other various legislative proposals impact your ability to share data among large and small suppliers alike? What clarifications are needed to ensure those supply chains aren't disrupted?

Answer. The CCPA allows a business to share personal information with its contracted service providers so the service provider can perform activities required under its contract. The CCPA also requires businesses to disclose the categories of third parties that receive personal information for a business purpose, such as with service providers. Some proposed legislation would modify these requirements to disclose the names of the service providers with which data is shared. If that service provider is an individual, such as a delivery driver, disclosing the names of specific service providers creates a risk to the privacy of another person's information.

Some proposed legislation includes language requiring a business to disclose the names of the service providers with which data is shared. If that service provider is an individual, such as a delivery driver, disclosing the names of specific service providers creates a risk to the privacy of another person's information. Additionally, legislative proposals should have strong language protecting the sharing of information with contracted service providers that also obligates service providers to protect personal information they receive.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TOM UDALL TO NUALA O'CONNOR

Enforcement is a critical component of any data privacy law, and State Attorneys General must play an important role ensuring that these laws are followed and consumers' privacy is protected.

Question. Should State Attorneys General have the ability to fully enforce a hypothetical Federal privacy law? And should State Attorneys General have the ability to enforce state privacy laws—as long as they are not in direct conflict with the Federal law?

Answer. Yes, Walmart supports both the Federal Trade Commission and State Attorneys General enforcing a Federal privacy law that preempts a patchwork of inconsistent state laws, which are insufficient to protect individual privacy and are inefficient for interstate commerce.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO MICHELLE RICHARDSON

New technologies have made it easier for people to monitor their health, but health tracking apps, wearable devices, and home DNA testing kits have given companies access to consumers' private health data, which is not protected under existing privacy law. I introduced a bill with Senator Murkowski to require the Department of Health and Human Services to address this issue.

Question. Do you believe that any new privacy regulations should cover sensitive health data that is not covered under existing Federal health privacy laws?

Answer. Yes, providing heightened protections for unregulated health information is one of the most important goals of a comprehensive privacy bill. Congress should broadly define this category of data to include information that reflects mental or physical health, wellbeing, or status on its face. It should also include any information that is collected, processed or shared for this purpose, regardless of the nature of the information or how it was created and collected.

We also recommend that Congress directly legislate in this space with substantive standards—such as a prohibition on the collection, use, and sharing of this data if it is not necessary to provide the service a consumer signs up for. Because this data is on the consumer market and the companies that collect the information are closer to traditional tech companies than health care providers, enforcement authority should reside with the Federal Trade Commission (FTC).

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO MICHELLE RICHARDSON

Enforcement is a critical component of any data privacy law, and State Attorneys General must play an important role ensuring that these laws are followed and consumer privacy is protected.

Question. Should State Attorneys General have the ability to fully enforce a hypothetical Federal privacy law? And should State Attorneys General have the ability to enforce state privacy laws—as long as they are not in direct conflict with the Federal law?

Answer. Yes, State Attorneys General should have enforcement authority in addition to any enforcement conducted by the FTC. According to a 2019 Government Accountability Office report, the FTC brought 23 enforcement cases against "unfair" data practices over the last decade.[1] With new privacy rules to more explicitly regulate corporate behavior, it is likely that a meaningful will be beyond the capacity of the FTC, even if it receives more resources. Additionally, state level enforcement will ensure that localized privacy violations will be redressed even if they do not rise to a Federal enforcement priority.

CDT prefers a single Federal privacy and security standard if it is sufficiently protective. We believe this can benefit both consumers and companies alike. However, preempting states from passing additional laws can only be justified by a Federal law that clearly prohibits the most egregious data practices. Because the breadth and depth of a preemption provision will likely be proportional to the substance of a Federal law, we look forward to working with your office to make sure that any preemption provision is properly calibrated.

○

[1] GAO, *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility,* Jan. 2019, available at *https://www.gao.gov/assets/700/696437.pdf.*