S. HRG. 116–661

SMALL BUSINESS PERSPECTIVES ON A FEDERAL DATA PRIVACY FRAMEWORK

HEARING

BEFORE THE

SUBCOMMITTEE ON MANUFACTURING, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MARCH 26, 2019

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
60–882 PDF WASHINGTON : 2025

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

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

SUBCOMMITTEE ON MANUFACTURING, TRADE, AND CONSUMER PROTECTION

JERRY MORAN, Kansas, *Chairman*
JOHN THUNE, South Dakota
DEB FISCHER, Nebraska
DAN SULLIVAN, Alaska
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD YOUNG, Indiana

RICHARD BLUMENTHAL, Connecticut, *Ranking*
AMY KLOBUCHAR, Minnesota
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
TAMMY BALDWIN, Wisconsin
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

CONTENTS

SMALL BUSINESS PERSPECTIVES ON A FEDERAL DATA PRIVACY FRAMEWORK

TUESDAY, MARCH 26, 2019

U.S. SENATE,
SUBCOMMITTEE ON MANUFACTURING, TRADE, AND CONSUMER PROTECTION,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:38 p.m. in room SD–562, Dirksen Senate Office Building, Hon. Jerry Moran, Chairman of the Subcommittee, presiding.

Present: Senators Moran [presiding], Blumenthal, Wicker, and Thune.

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

Senator MORAN. Good afternoon, everyone.

I call this subcommittee hearing to order.

Mr. Blumenthal, I'm sure, will be here shortly. We just had a vote, which is why I'm slightly late but embarrassingly late enough that the Chairman of the Full Committee beat me here, and I would not want to detain him any longer than necessary.

So, I'm going to give my opening statement. We'll see if Senator Blumenthal arrives and we'll go from there.

Welcome to today's hearing titled "Small Business Perspectives on a Federal Policy—I'm sorry—Federal Privacy Framework."

More and more questions and concerns have arisen from allegations of "unfair and deceptive practices" conducted by a variety of companies related to their handling of consumer personal information.

As the Subcommittee with oversight jurisdiction for consumer protection, we have sought specific answers to these questionable practices on many occasions in the form of public letters, stakeholder briefings, and hearings, stretching back to the prior Congress and before.

This subcommittee in particular has held hearings to evaluate troublesome industry practices, such as the Cambridge Analytica scandal, and other reports regarding the lack of privacy and security protections surrounding consumer data.

Additionally, the Subcommittee has sought direct input from the jurisdictional enforcement agency, the Federal Trade Commission, which we have jurisdiction over, and it is charged with enforcing the "unfair and deceptive practices in or affecting commerce," inclusive of consumer data privacy under Section 5(a) of the FTC Act.

Last November, we heard from all five FTC Commissioners on specific legislative actions Congress should take to better protect consumers from harmful business practices of bad actors and with over a hundred data security and privacy cases brought before them in the past 20 years, their feedback was greatly appreciated.

All of this proactive information gathering from industry, consumer advocacy groups, academics, and agency officials is intended to inform our legislative efforts to bolster consumer protections.

Additionally, given the implementation of the General Data Protection Regulation, GDPR, in Europe and the passage of the California Consumer Privacy Act and the likelihood of other states enacting their own consumer privacy laws, it is clear that the U.S. needs a Federal consumer data privacy law that provides clarity in an increasingly complex regulatory environment.

To that end, I've been working with the Ranking Member, Senator Blumenthal, along with other bipartisan members of our committee, including the Full Committee Chairman, Chairman Wicker, and Senator Schatz.

We've been attempting to identify responsible Federal privacy standards that provide clear and effective protection to consumers while also aiming to provide some regulatory certainty to businesses in the interest of creating jobs, promoting innovation, and competition in the global economy.

The focus of today's hearing is to emphasize the specific concerns of small and new businesses and how they utilize and protect consumer information within their operations.

These businesses have fewer resources in handling the complexities of increased regulatory privacy compliance and associated costs. However, it is also critical to highlight that not all small businesses are the same and consumer data offers different uses, challenges, and in some cases liabilities across the various models of small businesses and startups.

I look forward to hearing from the witness panel about what they think should be included in Federal privacy legislation and how new FTC enforcement authorities should account for the size and scope of a business processing consumer data, while also factoring in the sensitivity of that information and consumer harms associated with their practices.

Additionally, I'd be interested in hearing from the panel on how GDPR and the California Consumer Privacy Act specifically impact their operations or the operations of their member companies.

Joining us today is Ryan Weber, who serves as the President of the KC Tech Council. The Council serves as a regional advocate for Kansas City's tech industry, and while its members are comprised of companies in various sizes and models, Mr. Weber will provide a valuable perspective on behalf of the Council's small businesses in both Kansas and Missouri.

Second, Mr. Evan Engstrom, the Executive Director of Engine, will provide testimony on behalf of their association's startup members. Engine's membership covers a diverse group of sectors and models, and I look forward to hearing how privacy regulations could disproportionately affect startups which are oftentimes best positioned to innovate and drive competition.

Mr. Jeff England from Silver Star Communications is our third witness. He is based in Wyoming and will provide testimony from the perspective of a rural telephone and Internet service provider. Providing high-speed broadband to rural communities is a costly process, as many members on this subcommittee are well aware, and Congress must effectively account for expected compliance costs on small carriers associated with any Federal privacy bill if it is to be enacted.

Ms. Nina Dosanjh is a realtor working with the Nolan Group at Vanguard Properties in San Francisco, and she will provide insight to the unique needs and challenges facing small businesses in real estate as it pertains to our privacy discussion. Her role as the Technology Policy Committee Vice Chair for the National Association of Realtors make her exceptionally qualified.

Finally, Mr. Justin Brookman is the Director of Consumer Privacy and Technology Policy for Consumer Reports. As a former policy director of the FTC, Mr. Brookman will provide helpful insight to identify regulatory gaps in consumer privacy protection.

The distinctly unique perspectives of our witnesses today should provide valuable insight to our subcommittee's efforts in identifying an appropriate Federal privacy framework.

With that, I turn to the Ranking Member so that he can make his opening statement.

Senator Blumenthal, thank you.

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

Senator BLUMENTHAL. Thank you, Senator Moran.

And I want to firstly thank you for having this hearing and for being such a strong advocate and champion and my gratitude, as well, to Chairman Wicker.

We have a really significant and productive team, including Senator Schatz, and I am committed to moving forward in a very bipartisan way. This issue of privacy is of paramount importance and it should be of bipartisan significance.

Others on this committee and Judiciary, including Senator Klobuchar, have been leaders in this effort and I'm very heartened that they have been contributing. In fact, just a short time ago, we held a hearing in the Judiciary Committee and Senator Klobuchar and I are on both committees and I hope we can draw the best in support from both committees.

This hearing is very, very timely. One year ago this month, we learned that the political firm of Cambridge Analytica, now almost a household word in the tech community at least, had illicitly stolen data on tens of millions of Facebook users to manipulate our election. It was a wake-up call for the American public and it sparked a shift in our relationship with Big Tech.

Anyone who thinks their privacy is sacrosanct or well-protected is fooling themselves, and we need a privacy bill of rights, a set of protections that is no less stringent than the people of California enjoy, no less protective than the people of Europe have.

There's no reason that the people of the United States should be any less protected, whether you run a small business or you attend a daycare center. No matter what your age, no matter where you

go, you deserve that privacy, and we all carry in our pockets the most sophisticated tracking devices ever known to man. Our phones monitor our movements, our health, and even our family affairs.

Consumers could care less whether the company mining their data is a tech giant or a small business. They simply want to choose how that information is used or shared and small businesses could care less who is going to be protecting them as long as they receive that protection and it is guaranteed.

We see more companies, small and large, attempting to compete, actually contending with each other, on privacy. Earlier this month in the Judiciary Committee, we heard from DuckDuckGo, a competitor of Google Search. Its CEO told us that his company is both profitable and compliant with California's rules. It was ready because privacy was a foundational value to them and we need more companies like DuckDuckGo who have respect for privacy and succeed both in making money and also protecting their consumers.

Congress can set a baseline, a floor that establishes privacy as a right, really a set of rights, a bill of rights, and a business value. We can promote a market that enables companies to compete in offering the best privacy-friendly services rather than dumbing them down or punishing them.

So I look forward to crafting rules that accommodate the needs of small businesses, but we must raise the bar, not lower it.

I look forward to hearing how our markets can reflect those values, promote competition, and protect consumers. With the right balance, we can create new spaces for innovation and products that protect privacy.

So, again, I thank my Chairman, both Chairmen who are here today, and I think it reflects our bipartisan interests that we have this kind of turnout.

Thank you.

Senator MORAN. Senator Blumenthal, thank you very much for your opening comments, including those about the bipartisan effort to reach a solid conclusion, and I appreciate very much the way you've approached this and the good working relationship we have and a desire on the part of both of us to accomplish a goal of greater privacy for consumers.

None of this could be possible without the Full Committee Chairman, and I now recognize him for his opening comments.

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

Senator WICKER. Well, thank you very much, Chairman Moran and Senator Blumenthal.

I'm just here to add my words of support and appreciation for the leadership of this subcommittee. I will associate myself with the remarks of both the Chair and the Ranking Member of this subcommittee and appreciate their leadership and work and diligence and knowledge about this issue.

I think it's also clear from people who attended our Full Committee meeting and hearing several days ago that Ranking Member Cantwell of the Full Committee is a knowledgeable and diligent

participant in this issue and shares the same goals as the two previous speakers.

This is a priority for everyone on the Committee. It's something that must be done and it must be done on a bipartisan basis and so let's salute the small businesses of America. They innovate. They create jobs. They fuel the economy and economic development of this country, and they are very vibrant members of the local communities in Mississippi and Kansas and Connecticut and Minnesota, and we appreciate them.

As the Commerce Committee continues its work to develop a strong Federal data privacy framework that protects consumers and gives them more control over their data, it's important that any privacy law sustain and promote economic development among small business, which is, of course, the engine of so much job creation.

So I thank our members today. I thank both of my teammates at the leadership of this subcommittee for stressing the need for bipartisanship. Something of this magnitude will not, cannot possibly be done without strong bipartisan support both in the House and the Senate.

So I'm delighted to see the leadership proceeding today and I'm delighted to have our witnesses.

Thank you so much.

Senator MORAN. Chairman, I appreciate your opening comments and appreciate your leadership in the Full Committee and with us in trying to achieve that result.

We have votes at 4 o'clock. So the time is short. I would ask you all to keep your remarks to the 5 minutes under the rules and ask my colleagues to be able to ask and answer their questions within their 5 minutes.

With that, I recognize Mr. Ryan Weber, the President of Kansas City Tech Council.

STATEMENT OF RYAN WEBER, PRESIDENT, KC TECH COUNCIL

Mr. WEBER. Thank you, Mr. Chairman Wicker and Chairman Moran, and Ranking Member Blumenthal, and Committee Member Klobuchar. Thank you for inviting me to testify.

My name is Ryan Weber. I'm President of KC Tech Council. We're a non-partisan, nonprofit 5(1)(c)(6) organization, and we serve as a regional advocate for Kansas City's tech industry.

By the way, that industry in our metro area includes both Kansas and Missouri but also about 3,800 tech employers, about a 100,000 workers. They contribute about $11 billion to our economy. It's a big part of our business in our region.

And though we work with a lot of enterprise companies, my testimony today is provided on behalf of those small and startup businesses that comprise our member companies, like KC Tech Council, and like any other association president, in order to prepare for today's testimony, I asked many of those member companies and personally reached out to them, especially the small and startup companies, and asked them for feedback regarding the potential impact of Federal data privacy laws and for some of those companies, I want to be honest, they're just now learning about this issue at that small and startup level.

This is for some of them, this is new, and these are things they're currently educating themselves on, but they did have some very specific feedback, those who specifically do business in Europe and other places that may have had to focus on these issues.

There were a couple of themes. I'll share some of those real quickly. The unanimous theme was the importance of Federal preemption for the potential of a Federal data privacy law. They are concerned that if multiple states, like California and their CCPA law, if there's multiple states they have to comply with, obviously there's going to be a cost to that compliance. That could create entry of burden but also a barrier of entry for some of those companies.

Second, they're concerned about the impacts that GDPR and CCPA will have on their ability to innovate and leverage emerging technologies, and it often is those small companies that focus on some of those things, like artificial intelligence and block chain technologies, that would be dramatically impacted by Federal data privacy laws, and also that's really just what we know about today. You know, innovation happens very quickly and we don't know what the future brings, but data will be a part of that.

Third, the goal of any privacy law should be to prevent personal information from being used in harmful ways and not all data is the same and should be treated the same and considerations for how to enforce some of those different pieces of data in the Federal privacy law should be taken into account.

Enforcement is also of great concern amongst those business leaders and for GDPR and CCPA, enforcement can contain either millions of dollars or a percentage of revenue and for small companies or startup companies that would be essentially a death blow to those businesses.

In summary, the Federal preemption, future of innovation, what distinction on data will be met, those are some of the most important things, along with enforcement, that our member companies represent.

So thank you for the opportunity to testify today and represent Kansas City's tech industry.

[The prepared statement of Mr. Weber follows:]

PREPARED STATEMENT OF RYAN WEBER, PRESIDENT, KC TECH COUNCIL

On behalf of the KC Tech Council, our member companies and board of directors, thank you for the opportunity to testify about the potential impact future Federal privacy laws could have on small and startup tech firms. The KC Tech Council is a nonpartisan, nonprofit 501(c)(6) association serving as the regional advocate for Kansas City's tech industry. The organization is funded by regional tech employers and led by a board of directors consisting of 40 executives from enterprise level and small to medium-sized companies.

It has been my honor to serve as President of the KC Tech Council for the past seven years. My statement today has been formed by direct feedback from our member companies, board members and our Federal advocacy partners at CompTIA. Although the KC Tech Council's membership includes enterprise-level companies, this statement was created on behalf of companies with less than 500 employees.

FEDERAL PREEMPTION

A strong, preemptive Federal Data Privacy law is essential and supported by the KC Tech Council. In a recent survey of our members who identify as small or medium-sized tech firms, we asked:

"In regards to your business's ability to scale, how important is Federal preemption of data privacy laws rather than state-by-state laws, like California's CCPA?" Unanimously, the response to this question was; Very Important. Below are three examples why:

Unpredictable | Often, business leaders are expected to predict the future to grow their business. The recent passing of California's Consumer Privacy Act (CCPA) sent a ripple throughout Kansas City's tech industry and the business community. It will require a business to put a conspicuous "Do Not Sell My Info" link on its website and delete consumer information upon request, among other things. As other states follow suit and amend their privacy laws, tech companies will face countless and sometimes conflicting requirements. This regulatory uncertainty is a huge concern and a threat to small and startup companies. A reasonable Federal data privacy law will stabilize this threat.

This unpredictability can affect future investment, too. According to research conducted in the first six months after GDPR's implementation, overly prescriptive privacy laws can have a disproportionate impact on small businesses. Investment in startups and new tech companies in the EU has dropped since the GDPR went into effect in May,[1] while small businesses in Europe have lost market share to large companies in places like the ad tech sector in recent months.[2] Meanwhile, some U.S. websites have chosen to block EU visitors rather than spend the money required to come into compliance with GDPR.

Innovation | Artificial intelligence (AI), machine learning and blockchain are currently referred to as emerging technologies. These tools are complex, and only a small number of people in the world fully understand how to scale these applications successfully. The convergence of these tools with Big Data analytics helps businesses make better decisions, reduce costs and transform their business processes. Without access to this data, the continued investment in these and other new technologies may wane. As I will touch on shortly, a Federal privacy law can address consumer concerns by requiring transparency and notice of the algorithms, processing, and transfer of personal data.

GDPR and CCPA address an individual user's "right to be forgotten." In theory, this principle is worthy of attention. However, in practice, business leaders are concerned about the feasibility of recalling or deleting individual user data, specifically on legacy systems. It is possible deleting records could affect the future use of a database with emerging technology applications. This is a particular concern with blockchain technology.

GDPR also contains a purpose limitation that prohibits companies from using personal data for a purpose other than for which it was originally collected. While the goal of the purpose limitation, trying to limit the use of data, is noble, the result has been that companies are prevented from using their data for developing innovative new products, machine learning or AI. The U.S. should certainly place limits on the use of personal data, but it should provide flexibility for innovative uses as long as there is little or no risk of harm to users.

Cost | The evolving patchwork of state privacy laws places a significant legal and technological burden on small and startup companies. A 2017 Ponemon Institute Study found that the average cost of data protection compliance for multinational organizations had increased 43 percent from 2011, although the cost of non-compliance proved much greater.[2] The cost to build privacy-compliant software products, websites and applications are rapidly increasing, and the more regulatory masters there are, the greater the increase.

A state-by-state approach to data privacy creates a compliance nightmare for the entire tech industry, but particularly for small businesses with limited resources. Data does not abide by state boundaries, but each state has its own privacy law for its residents. As states create new and increasingly disparate privacy requirements, the result will prove untenable and could have a disastrous impact on small businesses and innovation.

It is not common for businesses to advocate for Federal regulation, but a Federal standard for data privacy is simply too important. Our support for a Federal law should reinforce the impact these laws have on the success of small and startup U.S. technology companies. Without Federal preemption, innovation may be slowed

---

[1] Jia, Jian and Jin, Ginger Zhe and Wagman, Liad, The Short-Run Effects of GDPR on Technology Venture Investment (November 5, 2018). Available at SSRN: *https://ssrn.com/abstract=3278912* or *http://dx.doi.org/10.2139/ssrn.3278912*

[2] Fifth annual survey shows a significant spike in legal defense spending while breaches involving third-party organizations remained the most costly *https://www.ponemon.org/news-2/23*

or altered in order to comply with state laws, and the cost to comply may put some small and startup companies out of business.

STATUTORY CONSIDERATIONS

In today's economy, personal data is a valued asset for almost every business, and for many, the most valuable asset. Using other information from data brokers, companies can now narrowly target their prospects and customers in ways we could not imagine five years ago.

In this tension between commerce and privacy, we believe transparency is key. Companies should know how they collect, use, store, secure and share personal data, and be accountable for it. We believe a Federal law can embrace the principles of data privacy and still keep the regulatory burden within reason for small to medium-sized businesses.

Privacy | A Federal privacy law should ensure that businesses only use personal data for legitimate purposes, and disclose those uses and purposes. Businesses should not make new and different uses of personal data without consent or a similar justification. They should collect only the personal data they need, and not keep it longer than they need it. They should take reasonable measures to protect the data, and have a way for people to correct inaccuracies. They should provide notice in the event of a breach.

> *"If a new Federal law can help move the EU to view our privacy protections to be "adequate," we may be able to avoid some serious obstacles to data transfer and online commerce created by GDPR."—Tedrick Housh, Data Privacy attorney at Lathrop Gage, Kansas City, MO*

Collection and Use | How data is collected and used are already set forth in most companies' privacy policies and terms & conditions. In some cases, data is sold to generate revenue and sell advertisements. The process by which data is sold, and for what intent, should be transparent.

The goal of any privacy law should be to prevent personal information from being used in ways that harm individuals. New Federal privacy law should not contain absolute restrictions on the collection of data or include non-personal data within its ambit. GDPR, for example, includes publicly available IP addresses as "personal data." The risk of harm to individuals from possessing these types of data is extremely low. If a company is transparent about the fact that it will not re-identify its aggregated, anonymized and/or encrypted data, and abides by that commitment, it should not be subject to the same fines and other enforcement as a company that is not transparent.

Storage | The databases used to store collected information are complicated and connected, whether on-premises or in the cloud. Some data is used often and necessary for business operations. Other data sets, without immediate or functional need, are nonetheless a source for research or technological advances. Mere storage of personal data, without misuse or lack of security standards, should not result in liability.

Security | Threats to company data are not only constant; they are constantly changing. Security is not "one size fits all." No matter who has it, sensitive data (like genetic or medical information) should be subject to enhanced protection, boosted by more frequent penetration testing, cybersecurity audits, and other measures. Otherwise, we believe companies securing ordinary personal data could be subject to a "reasonableness" standard that takes into account the company's particular industry, financial means, and size.

Portability | Data portability is a two-way street. Just as consumers increasingly expect their personal data to be portable, like a cell phone number, companies should be able to transfer such data in its possession in a merger or acquisition. So long as a company has been transparent in how it shares data with third parties, it should be able to share or sell personal data without fear of violating the law.

ENFORCEMENT

Accountability is an important aspect of meaningful data privacy law. GDPR and CCPA include predetermined levels of fines, which reach into the millions of dollars or a percentage of revenue, whichever is higher. Fines at this level could mean the end for small and startup companies. An executive from one of our member companies weighed in on this subject:

> *"The law should not be so broad that it allows big companies like Facebook or Amazon to sell personal data but not so onerous that smaller businesses incur*

large costs to be compliant."—Jeanette Prenger, CEO of ECCO Select, Kansas City, MO

Another potential death blow to small to medium-sized businesses is a data breach class action lawsuit. Even with little or no proof of identity theft or other injuries to the consumer class, courts are letting these cases proceed. A new Federal data privacy law could define the type of tangible proof of actual harm to give standing before a court.

CONCLUSION

Algorithms are the backbone of most modern technology applications, and algorithmic thinking is necessary when considering the future of Federal data privacy laws. Conditional algorithms use IF–THEN decisions between two courses of actions. For example, IF a company, no matter the size collects sensitive data, THEN it must comply with Federal data privacy laws and meet certain cybersecurity standards set forth by the appropriate regulatory agency.

As technology continues to advance and find its way into every industry, business sector, and company, we must remember, not all technology is created equal and not all data should be treated the same.

Accountability will make Federal data privacy laws effective. The agency responsible for upholding these laws should be allowed to adjust fines and penalties equal to the violation. This sentiment is shared by our member companies. Other global examples of privacy laws, such as General Data Protection Rights (GDPR), set fines at such a high-level many small and startup companies cannot afford.

We believe small to medium-sized tech companies are already defining and creating the jobs of the next generation. Thank you for the opportunity to present the KC Tech Council's views on how to promote that growth and respect data privacy at the same time.

Senator MORAN. I would point out that if Kansas and Missouri can cooperate as well as they do in the Kansas City Tech Council, Republicans and Democrats can reach a conclusion——

Mr. WEBER. Yes, sir.

Senator MORAN.—on this legislation.

Mr. WEBER. Let's hope.

Senator MORAN. I believe it.

Mr. Engstrom.

STATEMENT OF EVAN ENGSTROM, EXECUTIVE DIRECTOR, ENGINE ADVOCACY AND RESEARCH FOUNDATION

Mr. ENGSTROM. Chairman Wicker, Chairman Moran, Ranking Member Blumenthal, Members of the Subcommittee, thank you for inviting me to testify on the impact of consumer privacy protections on U.S. startups.

Engine is a nonprofit that works with a network of startups throughout the country to push for policies that promote entrepreneurship and right now, consumer privacy regulation is a priority for many small businesses.

Congress must create robust uniform rules that provide transparency and user choice while directly prohibiting abusive practices. A strong Federal bill will increase consumer confidence and protect our thriving startup ecosystem.

If carefully crafted, national rules can avoid imposing the significant costs associated with state-by-state regulation that would make it all but impossible for startups to compete with larger companies.

For startups, user privacy is more than a buzzword. It's a business imperative. With every headline-grabbing misstep by an Internet giant, consumers lose trust in the online economy. It's the small startups without name recognition or longstanding relation-

ships with users that consumers will abandon first when trust is lost.

We already see startups using privacy as a competitive advantage, recognizing that they have to work harder to earn user trust. A strong Federal privacy law that shores up consumer confidence in the Internet ecosystem benefits users as well as competition.

At the same time, as state and Federal policymakers look to bolster privacy protections for consumers, there is a very real risk of creating a complex regulatory landscape that startups on bootstrap budgets can't afford to navigate.

We saw this in Europe after the General Data Protection Regulation was implemented last year and companies, from major U.S. newspapers to tiny tech startups, had to shut down access to European users.

We anticipate similar things will happen when California's new privacy law, the California Consumer Privacy Act or CCPA, goes into effect in 2020.

To be clear, we fully support CCPA's goals. Consumers should know what types of data companies collect and how that data is shared. But what's poised to go into law next year will have unintended consequences for startups.

CCPA creates an overbroad set of definitions and obligations that large companies will be able to manage but startups will not. In the rush to pass CCPA, the California Legislature inadvertently produced a bill full of typos, contradictions, and unworkable provisions that in some cases will actually discourage pro-security best practices and will require companies to collect more personal user data.

For example, the law's nondiscrimination and data deletion provisions will require companies to collect sensitive personally identifiable information, such as credit card and social security numbers, that they previously had no interest in gathering, and while CCPA implicitly recognizes that it will pose undue burdens on smaller companies, the law's small business exemption fails to protect most of the California startups that are creating jobs and providing innovative services to consumers.

Beyond our specific concerns with CCPA's provisions, the risk of every state adopting its own privacy laws will make it even more difficult for startups to compete with large incumbents.

As each new state law goes into effect, startups will be faced with an increasingly complex and potentially conflicting set of requirements and obligations when it comes to how they can collect, use, store, and share consumer data.

Even if state laws are relatively consistent, small variations multiplied over 50 jurisdictions will create insurmountable administrative hurdles for all but the most well-funded companies.

No matter how similar any state privacy laws are, startups will almost certainly have to renegotiate all of their vendor contracts to cover compliance with each new law.

Unlike massive Internet companies that can build most of their services in-house, startups rely on a range of external vendors to run day-to-day business processes, from cloud storage to cybersecurity tools to back-end web posting. These administrative

burdens have little impact on consumer welfare and will fall disproportionately on small companies.

Fortunately, Congress is fully equipped to address these concerns. A single strong Federal standard can ensure equal protections for users across state lines while avoiding unnecessary burdens that put honest startups at a competitive disadvantage.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Engstrom follows:]

PREPARED STATEMENT OF EVAN ENGSTROM, EXECUTIVE DIRECTOR, ENGINE ADVOCACY AND RESEARCH FOUNDATION

I. Introduction

Chairman Moran, Ranking Member Blumenthal, members of the subcommittee. Thank you for inviting me to testify on the role of consumer privacy protections in the U.S. startup ecosystem.

Engine is a non-profit that works with a network of startups across the Nation to push for policies that advance the startup ecosystem, and right now, consumer privacy is at the top of mind for many small and new companies.

For startups, "user privacy" is more than just a regulatory concern or buzzword, it's a business imperative. With every headline-grabbing misstep by an Internet giant, consumers lose trust in the Internet economy. It's the new, small startups without name recognition, longstanding reputations, or relationships with users that consumers abandon first when that trust is lost.[1] We already see startups using privacy as a competitive advantage, recognizing that they have to do more with less in order to maintain users' trust. A strong Federal privacy law that shores up consumer trust in the Internet ecosystem benefits consumers, as well as startups.

At the same time, as state and Federal policymakers look to bolster privacy protections for consumers, there is a very real risk that the end result will be a complex regulatory landscape that startups on bootstrap budgets can't afford to comply with, especially compared to large companies with massive budgets and legal teams. Rules that are ostensibly pro-privacy could end up cementing the market power of those very Internet giants whose behavior sparked much of these conversations.

We've seen this with the European Union's General Data Protection Regulation, where many small companies left European markets or abandoned plans to expand to European markets rather than face the costly compliance burdens.[2] In fact, there's concrete evidence that GDPR gave the big Internet companies a boost in Europe. According to one survey, Google's ad tracker actually saw an increase, albeit small, in reach since GDPR went into effect ten months ago.[3] Facebook's ad tracker saw a small decrease, but everyone else saw significant losses. GDPR's extensive and complex obligations created new compliance burdens that large incumbents could bear but resource-constrained startups could not. Policymakers should enshrine consumer privacy protections in law, but they must work to ensure far-reaching rules promote consumer welfare without harming competition.

Startups and consumer advocates are aligned in support for strong, commonsense privacy legislation. A robust, uniform set of rules that provides transparency and user choice while directly prohibiting abusive practices will increase consumer confidence and, if crafted carefully, can avoid imposing significant costs that will allow large Internet companies to grow their market share while smaller competitors struggle to cover compliance costs.

II. Congress should enshrine and build off of the goals of CCPA

We appreciate the goals of the California Consumer Protection Act, as well as the ballot initiative that preceded the law. Consumers should know what types of data companies have about them and how that data is shared. These goals are important and will shore up consumers' trust in the Internet ecosystem, which will help startups grow.

---

[1] PricewaterhouseCoopers, *Consumer Intelligence Series: Protect.me,* November 2017, available at: *https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf.*

[2] Hannah Kuchler, *US Small Businesses Drop EU Customers Over New Data Rule,* Financial Times, May 23, 2018, available at: *https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.*

[3] Björn Greif, *Study: Google is the Biggest Beneficiary of the GDPR,* Cliqz, Oct. 10, 2018, available at: *https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.*

While CCPA's objectives are laudable, the process leading to its passage was not. Although the ballot initiative's authors clearly spent considerable time on their proposal, the legislature spent less than a week translating the initiative's general ideas into actual bill text. As a result, California legislators were unable to fully evaluate the bill, its impact on California's startup community, or its actual value to consumers. This rushed process resulted in a well-intentioned law that is full of typos, contradictions, security loopholes, and vague obligations.

We've previously laid out our concerns about the unintended consequence of the language in CCPA.[4] The definitions in the law—specifically of "personal information" and "sale"—are so broad that they will sweep in everyday business practices small companies rely on. Its requirement that companies offer the same services to everyone regardless of consumers' privacy choices would force startups to build and maintain different business models based on different consumer privacy choices, no matter how costly to their operations. The law creates a right for a consumer to access the data a company has on her, but as currently written, it would force companies to choose between collecting more and highly sensitive information from consumers or risk complying with fraudulent access requests. The private right of action in the event of an "unauthorized disclosure" and statutory damages established by the law will create potential litigation costs that would devastate a small company. The law claims to carve out small businesses, but the exemption as written would fail to capture many California startups that are creating jobs and providing innovative products and services to consumers. While policymakers continue to refine aspects of CCPA at both the legislative and regulatory levels, several provisions that are currently set to go into effect next year will create burdens that will disproportionately impact startups.

A. Definition of sale. One of CCPA's central principles is the right of consumers to opt out of the sale of their personal data. Stated in the abstract, this may seem like an unobjectionable idea, but CCPA's implementation of this concept reveals some serious problems. For one, CCPA defines "sale"[5] expansively, covering many commonplace practices that businesses rely on to provide goods and services to consumers. Specifically, the bill says that "releasing, disclosing, disseminating, making available, transferring, or otherwise communicating. . .a consumer's personal information . . . to another business or a third party for. . .valuable consideration" constitutes a "sale" of data. It's not clear what is included by "valuable consideration," and we've heard from companies that routine data sharing that presents no meaningful privacy harms could be included in the definition of sale due to the vague "valuable consideration" language. For example, we've heard from a local delivery platform that sharing order trends with local merchants to help those retailers stock their shelves in accordance with consumer demand could constitute a "sale" of consumer data under the law, even if none of the shared data is connected with any individual consumer.

The definition of sale does exclude some consumer data transfers to service providers, but the exemption[6] provides limited protections because it relies on the narrow definitions of "service providers"[7] and "business purposes"[8] and prohibits service providers from retaining or using the data. This will severely limit the ability of startups to rely on third party vendors to run their business processes. Unlike large companies, which typically have the resources to build these capacities in-house, startups rely on outside vendors for everything from data processing, to analytics, to payment processing. We've already heard from companies who have trouble finding third-party vendors that provide necessary analytics services and can comply with the requirements laid out in CCPA.

B. Definition of personal information. Any sensible consumer privacy bill should recognize that different pieces of information raise different privacy concerns. Collecting information about a user's favorite color does not pose the same risk as collecting her social security number. In attempting to protect consumers' data from unreasonable exploitation, CCPA relies on an overly broad definition of "personal information"[9] that would cover virtually all information related in

---

[4] Engine, *Comments re: Implementing Implementing Regulations for the California Consumer Privacy Act,* March 8, 2019, available at: *https://www.engine.is/news/category/engine-files-comments-to-california-ag-on-state-privacy-law.*

[5] Cal. Civ. Code § 1798.140(t)(1).

[6] Cal. Civ. Code § 1798.140(t)(1)(C).

[7] Cal. Civ. Code § 1798.140(v).

[8] Cal. Civ. Code § 1798.140(d) et seq.

[9] Cal. Civ. Code § 1798.140(o) et seq.

any way to an individual user, no matter how sensitive or innocuous. Under CCPA, any "information that . . . relates to, describes, is capable of being associated with . . . a particular consumer or household" is deemed "personal information" and subject to the full protections of the law. It also includes a long list of specific pieces of information that are included in the law's definition—such as commercial information, "information regarding a consumer's interaction with an . . . application," and "inferences drawn" from other personal information—and gives the state Attorney General the authority to add more. It's difficult to imagine any piece of user information that does not "relate to" or is not "capable of being associated with a particular user."

Additionally, the definition does not explicitly carve out deidentified and aggregate consumer information, despite rigorous requirements around what constitutes deidentified data.[10] Taken together, the vast definition of personal information will increase the scope of the law, require companies to allow consumers to opt-out of harmless data collection and sharing, and dramatically increase the burden companies face when consumers exercise their rights to access and delete data about them without any clear consumer benefit.

C. Prohibition on differing service based on consumer privacy choices. CCPA prohibits companies from offering different prices or levels of quality of products and services to consumers who exercise their rights under the law, including the right to opt-out of data sharing.[11] In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups. Unlike large Internet companies that have been offering ad-supported free services for years, a startup entering the market will have a harder time getting new users who are unfamiliar with the company to pay for its products and services. Even if a startup can get some users to pay, the law would effectively require every ad-supported company to take on the burdens associated with establishing a payment processing system in case some users decide to opt-out. At the same time, a small company will have significantly fewer opportunities to offset the costs of offering a product or service for free using revenue streams from other parts of its business, while bigger companies are better positioned to take a loss on offering a free product or service.

The law does allow companies to charge a different rate or offer a different level of products or services so long as "that difference is reasonably related to the value provided to the consumer by the consumer's data."[12] While this phrasing is likely a drafting error and obviously unworkable—how could a company know how much an individual consumer values his own data?—even a generous reading of the law's presumed goal would present existential problems for small startups. Even if companies are forced to provide service to consumers who opt-out of data sharing practices that are fundamental to the company's business model, but are allowed to recoup the lost value directly from consumers by charging a different price or offering a different level of service so long as that difference is reasonably related to the value provided to the *company* by the consumer's data, startups would have a very difficult time estimating or defending in court what would constitute a price or quality difference that's "reasonably" related to the value of a consumer's data. As startups launch and grow their businesses, there's typically not an immediate, obvious value that can be clearly assigned to individual pieces of data supplied by consumers. Even if a data set has an explicit value in the eyes of investors, data associated with any particular consumer typically does not hold much value on its own.

Even worse, this non-discrimination provision would require every company that shares user data to build the infrastructure to process customer payments in the off chance that a particular consumer opts-out of the company's data practices but wishes to pay a "reasonably related" fee instead. Larger companies might be able to bear the increased overhead of payment processing, but smaller startups will not.

D. Privacy and security problems with CCPA's right to access and delete. CCPA mirrors GDPR in that it attempts to provide consumers with a right to access and delete the personal information companies have about them. These rights, in and of themselves, are a crucial part of consumer privacy protections, but they need to be reasonably cabined to prevent unintended burdens for compa-

[10] Cal. Civ. Code § 1798.140(h) et seq.
[11] Cal. Civ. Code § 1798.125 et seq.
[12] Cal. Civ. Code § 1798.125 (a)(2).

nies. The law provides reasonably broad exceptions for when a company does not have to complete a consumer's request to delete data, but the law should be more inclusive of practices that build in privacy protections by design, such as data minimization, aggregation, and using synthetic data. If a company has deidentified a data set or used an existing data set of personal information to create artificial data that mimics the characteristics of the real data set, it could lose the ability to "delete" a consumer's data once it has been baked into an aggregate or synthetic data set. Requiring companies to do so could actually force them to collect additional consumer personal information and reidentify the data. For some immutable data structures like blockchains, deleting user data may be technically impossible.

Of greatest concern is that the law requires companies to comply with "verifiable" consumer requests for data. While the exact requirements are expected to be fleshed out in the Attorney General's rulemaking, the law prohibits companies from requiring users to create an account in order to submit a verifiable request.[13] This restriction makes sense when talking about data brokers with whom most consumers don't directly interact, but consumer-facing companies should explicitly be allowed to require users to sign in to their accounts to make such requests. Otherwise, companies will have to collect significantly more personal information to verify that a person requesting a consumer's data is, in fact, that consumer or run the risk of disclosing a consumer's personal information without their consent.

E. Private right of action in the event of a data breach. CCPA creates a private right of action that will let consumers bring lawsuits against companies that suffer from "an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures," and the law sets the damages at "not less than one hundred dollars and not greater than seven hundred and fifty per consumer per incident."[14] Putting aside the question of what constitutes an individual "incident" in the context of a data breach, the vague language included in this provision—especially "unauthorized access. . .or disclosure" and "reasonable security procedures"—will create uncertainty for startups that will ultimately be decided inconsistently in the courts. No matter how thorough a company's data security practices are, determining whether they were legally "reasonable" is not amenable to early adjudication in a lawsuit. As such, data breach litigation is a lose-lose proposition for startups: settling, paying a damages award, or even litigating a case to victory will likely bankrupt most early-stage companies, as CCPA does not envision attorneys' fees awards to the winning party. The availability of significant statutory damages wholly unrelated to any actual harm suffered creates financial incentives for any individual implicated in a data breach to bring a lawsuit, since startups will almost always be better off settling a lawsuit rather than paying a statutory damages award or incurring legal costs to dismiss a meritless claim.

F. CCPA's small business exemption fails to capture startups. We appreciate the California legislature's attempt to carve out small businesses from the onerous burdens imposed by the CCPA, but the law sets the threshold for businesses so low that few companies with users in California will qualify. The law creates three requirements to be considered a small business: a company must have less than $25,000,000 in annual gross revenues, make less than 50 percent of its annual revenues from the sale of personal data, and handle data relating to fewer than 50,000 consumers, households, or devices. In practice, setting the threshold at 50,000 consumers, households, or devices will quickly sweep in small Internet-based companies whose products and services are accessed from multiple devices. For instance, if each consumer visits a website that tracks unique visitors from a smartphone, a personal computer, a work computer, and a tablet, the 50,000 figure quickly drops to under 13,000 "users or devices." At the same time, the law doesn't include an on-ramp, meaning that a startup that suddenly becomes popular could immediately find itself in violation of the law.

Ideally, a privacy law would be clear, straightforward, and consistent enough that companies of all sizes can afford to comply, especially recognizing that even a small company can create privacy harms depending on the sensitivity and scope of the consumer data it handles. However, the many burdens created by CCPA outlined above that have little to do with actually protecting consumer privacy highlight the need for small business protections when privacy laws

[13] Cal. Civ. Code § 1798.100(d).
[14] Cal. Civ. Code § 1798.150 et seq.

start with good intentions but end up with drafting errors and unintended consequences.

We hope to see these issues and more addressed as California lawmakers and the state Attorney General continue refining and clarifying the law. But the mere fact that the law is still so ambiguous in so many ways with the 2020 implementation date closing in makes it even more burdensome for startups that will struggle to become CCPA compliant on such a short timeline. Many of the companies that we work with are forced to put off planning for CCPA compliance until the law and regulations are more settled, and even the biggest startups will have to budget for outside consultants to help shape their compliance strategies. Unlike GDPR—which, despite its costs and consequences, gave companies two years to come into compliance—the CCPA enforcement date looms while the law's requirements are still in flux. If the thoroughly debated rules under GDPR still cost companies significant time and resources to comply with, the compliance costs will be even higher in light of the short timeline and rushed process for CCPA.

III. A single, Federal standard is better for startups and better for users

Beyond our specific concerns with CCPA's provisions, the risk of every state adopting its own privacy laws will make it even more difficult for startups to compete with large incumbents. As each new state law goes into effect, startups will be faced with an increasingly complex—and potentially conflicting—set of requirements and obligations when it comes to how they can collect, use, store, and share user data. Even if state laws don't differ dramatically, small variations multiplied over 50 iterations will create insurmountable administrative hurdles for all but the most well-funded companies. For example, putting aside differences in specific data collection practices that each state will regulate, each jurisdiction is likely to have slightly different requirements for transparency policies, user data correction or deletion requests, and reporting obligations.[15]

Additionally, even if two state privacy laws are virtually identical, startups will almost certainly have to renegotiate all of their vendor contracts to cover compliance with each new law. Unlike massive Internet companies that can build most of their services in-house, startups rely on several—sometimes dozens—of vendors to run the day-to-day processes that keep the business running, including cloud storage, payment processors, and backend website hosting. With every regulatory and legislative update requiring downstream compliance, startups have to redo contracts with each vendor to ensure they're not inadvertently and unknowingly running afoul of the law. We've heard from startups that the contract revisions required for GDPR compliance alone created significant costs for companies, and we expect CCPA compliance to be no different. Startups can't afford to spend the time and money do this again for every state, and it's hard to see how the value to consumers of 50 slightly different state laws would outweigh the resulting costs to competition and innovation.

A single, strong Federal standard written into law by Congress can ensure equal protections for users across state lines while saving startups the cost of having to comply with differences in state laws that, at best, all get at the same consumer protections in different ways.

IV. Components of a strong Federal law

A single, strong Federal law that preempts state laws is necessary to avoid the specific problems with CCPA and the broader anti-competitive impacts of state-by-state privacy regulation. There have been several Federal legislative proposals introduced in recent months that contain provisions that would address these concerns and bolster consumer privacy without harming innovation or competition. We appreciate lawmakers' thoughtful and deliberate approach on those proposals, including the several bills introduced by members of the committee. As Congress continues to consider privacy legislation, the following proposals can be incorporated in a way that protects consumers without placing undue burdens on small companies.

A. Right to access, correct, and delete. Engine supports lawmakers' efforts to provide consumers with a way to access, correct, and delete their data when it's held by companies. Consumers have a right to know what kinds of data companies collect and share, and they should be able to correct inaccurate data and

[15] CCPA requires companies to provide detailed reports to any user who sends a "verifiable consumer request," but the law leaves it up to the California Attorney General to determine how a company must verify the identity of a user making a request. §§ 1798.100(d), 1798.140(y) In the absence of Federal preemption, companies will have to create separate systems to comply with every state's unique process for verifying and responding to user requests.

disengage with a company by deleting their data. But it's important that these rights be balanced to reflect the ways that companies store and use data. If a company aggregates and deidentifies consumer data, uses real consumer data to create synthetic data sets, or uses customer data to train machine learning applications, there will be technological limits on how much the resulting data can be accurately connected back to individual consumers. Requiring companies to re-identify individual consumer data so they can comply with consumer requests to access, correct, or delete their data would end up forcing companies to collect even more user data, undermining the central purpose of privacy legislation.

B. Consumer controls over sharing data with companies. Engine supports giving consumers control over their data through a notice and consent regime with robust transparency and accountability requirements. At a high level, a Federal privacy law should be careful to craft notice and consent requirements so that they don't create large obstacles to data collection—either with an opt-in mechanism or an onerous opt-out mechanism—that would harm startups' ability to collect the data they need to provide the products and services they offer. If new legislation unreasonably limits the collection of non-sensitive data, startups will be structurally prevented from competing with large Internet companies in areas that require access to data sets, like machine learning, as more established platforms have already generated these data sets over years of operation.

While meaningful user control over how companies collect and share data should be central to any Federal privacy law, startups should not be forced to create new subscription-based services if some users choose to opt-out of their data practices. Startups should be permitted to compete on their chosen features and privacy practices and not forced to create an alternative service alongside their core product to reflect idiosyncratic consumer data choices. The costs associated with the non-discrimination provisions in CCPA and several Federal proposals would make it significantly harder for startups to compete with large incumbents that have the resources to offer both ad-supported and subscription-based products or the brand equity to switch to a completely fee-based service. As long as a company's data practices are made clear to consumers in a truly understandable and transparent manner, startups should be able to require that consumers provide certain information in order to access the service if that information is necessary for the company to provide the service it wants to offer. For instance, if a startup publishing platform wishes to distinguish itself from larger rivals by offering a more curated product that recommends articles to users based upon an internal recommendation engine, it will need to track consumer reading habits within the website to provide reading recommendations. Allowing users to opt-out of this data collection practice while still receiving access to the core product will make it impossible for the startup to offer the service it believes will help it compete with larger incumbents. We appreciate that some Federal proposals have addressed this concern by allowing companies to require consumers provide certain data—or allowing companies to deny service in the absence of the consent to collect that data—if the data is necessary to the company's operation.

C. Heightened protections for truly sensitive data. Engine supports increased user control over personal data with robust transparency and accountability requirements, but there are certain types of data that could present heightened privacy harms, and it makes sense to treat the collection, use, and sharing of that specific data differently under the law. However, it's important that the definition of sensitive data under the law be limited to truly sensitive information, such as precise geolocation information, government-issued identification numbers, biometric information, health information, financial information, etc. In instances where companies want to collect truly sensitive information, consumers should have the ability to opt-out without being denied access to the service or forced to accept a different level of quality of service. The only exception to this should be if the company truly needs the data to perform the service the customer is requesting. For instance, a mapping application needs a user's precise geolocation information to provide navigation directions as requested by the user. However, a flashlight app has no clear functional need to access a user's precise geolocation information to deliver its service to a consumer, and even if that flashlight app wanted to serve relevant advertising based on a user's location, it could target ads using more general, less sensitive data such as region or zip code.

D. Restrictions on objectionable uses of data. Under a notice and consent regime with robust transparency and accountability requirements, Engine would sup-

port additional restrictions on specific uses and sharing of data if those restrictions are targeted at activities that present increased potential privacy harms. For instance, we would support a prohibition on using consumer data related directly or indirectly to race, age, gender, and other protected characteristics to make decisions about finance, housing, or employment opportunities, including serving advertisements about finance, housing, or employment opportunities.

E. FTC rulemaking and enforcement around a Federal standard. If a Federal privacy law creates a uniform nationwide standard, Engine would support Congress giving the Federal Trade Commission the authority to write rules to implement the law and bring civil penalties to enforce the law. We would like to see the FTC's resources increased to meet that kind of demand. If Congress is considering giving state attorneys general the authority to enforce the Federal standard, there should be some requirement that the attorneys general coordinate with the FTC to ensure consistent enforcement of a predictable Federal standard.

V. Conclusion

Congress has a chance to build up from the California law by creating a single, Federal standard for privacy that protects consumers regardless of where they're located, avoids competition-and innovation-limiting pitfalls, and encourages good data hygiene for companies of all sizes. While the trope of a young startup CEO coding an ingenious app out of a garage or dorm room with little regard for its users' privacy has pervaded popular culture, the U.S. startup ecosystem is full of companies working in good faith to protect the privacy and security of their users. Congress should strive to create a Federal privacy framework that protects consumers without imposing unnecessary burdens that put honest startups at a competitive disadvantage to large incumbents.

Senator MORAN. Thank you very much.

Mr. England.

STATEMENT OF JEFFERSON ENGLAND, CHIEF FINANCIAL OFFICER, SILVER STAR COMMUNICATIONS

Mr. ENGLAND. Well, Chairman Moran, Ranking Member Blumenthal, and other Members of the Committee, my name is Jeff England, and I am the Vice President and Chief Financial Officer at Silver Star Communications, and I would like to just thank you all for the opportunity to be here today.

Silver Star Communications is headquartered in Thayne, Wyoming, which is right along the Idaho and Wyoming border. We are a small telephone and Internet service provider. We service nine rural counties that covers about 17,000 square miles in our area.

We are both an independent local exchange carrier providing regulated telephone services and a competitive local exchange carrier delivering some of the most cutting-edge Internet services that are available today.

Our company was formed in 1948 with the purpose of connecting our rural farmers in the mountain valley in which we live. It's humbling to remember that while we now celebrate being the first company in both Idaho and in Wyoming to deliver one gigabit residential Internet service, we once delivered basic telephone service along the top wire of a barbed wire fence.

We've seen significant changes in our industry from the days when a trouble ticket consisted of determining who is moving cows that day and forgot to reconnect the jumper at the gate and the largest privacy concern was that which was inherent with making a call on a party line.

What hasn't changed in our company's 71 years of existence is our customers' requirements for privacy and security. Because of this, we have adopted practices designed to maintain the privacy

of our customer data. We do not sell customer data and we do not collect and use customer data for the purposes of advertising or click revenue.

We have chosen not to collect and monetize this information as a competitive differentiator. So I appreciated what Mr. Engstrom just had to share about that topic. And by choosing to not collect this information, we believe we've established trust in our interactions with our customers.

We've also observed general trends in online services to suggest that the market is responding to customers' desires for increased protection with regards to their data.

Ranking Member Blumenthal, I had the same observations about DuckDuckGo, the web browser, and there's an example there and we choose to do the same, building a business model around not collecting that kind of data.

It is our position that any legislation considered by this committee should not limit the capability of a service provider to differentiate on the basis of privacy protection practices. Because we already do not collect and monetize customer information, we do not anticipate online privacy legislation to be overly burdensome so long as it meets certain criteria, and I've provided a number of suggestions in my written testimony, but with the time constraints that we have today, I'd like to focus on maybe our top three.

First, there must be consistent application of privacy protections. Legislation should establish consistent privacy protections that are technology-neutral and apply uniformly to companies that collect, use, or share consumers' online personal data.

We believe it's not necessarily who collects the data that the legislation should apply to. It, rather, is what kind of data that we might collect and what we do with the data that we collect that should be of concern.

Second, we believe that the pathway to success is built upon a Federal privacy framework that preempts state privacy laws.

We provide services in multiple states and having to manage a patchwork of state privacy laws will not only create an environment of uneven protections, but would create administrative burdens on small businesses and in my particular case draw very limited resources away from building out rural deployments of broadband services to the customers that we provide.

Third, there must be a single Federal agency identified with the responsibility to enforce the national privacy framework. Failure to do so would result in inconsistent requirements, uneven protections, and competing priorities.

We believe that the Federal Trade Commission should have exclusive authority to enforce privacy protection laws at the Federal level with State Attorney Generals having the authority to enforce the new Federal law.

This will allow for consistency in privacy legislation across all industries and companies as well as provide a framework for new businesses and industries to operate within.

As a rural Internet service provider, we would add that the FCC should expressly be precluded from having authority to enforce privacy protection laws. Failure to prohibit the FCC from enforcing

privacy protection requirements would endanger the deregulated status of Internet services that are being provided.

In conclusion, I would just like to say that as a small business, we love the opportunity to serve our customers and we know that we all share that same common interest of privacy protection and I appreciate the ability to spend some time with you here today.

[The prepared statement of Mr. England follows:]

PREPARED STATEMENT OF JEFFERSON ENGLAND, CHIEF FINANCIAL OFFICER, SILVER STAR COMMUNICATIONS

Chairman Moran, Ranking Member Blumenthal, and other distinguished Members of the subcommittee. My name is Jeff England, and I serve as the Vice-President and Chief Financial Officer of Silver Star Communications.

Silver Star Communications, headquartered in Thayne, WY, is a small telephone and Internet service provider, serving nine rural counties, comprising 16,922 square miles, located along the Western Wyoming and Eastern Idaho state border. We are both an independent local exchange carrier, providing regulated telephone services, and a competitive exchange carrier, delivering some of the most cutting-edge Internet services available today.

Our company was formed in 1948, with the purpose of connecting rural farmers in the mountain valley in which we live. It is humbling to remember that while we now celebrate being the first company in both Wyoming and Idaho to deliver gigabit Internet service to residential customers over a robust fiber optic network, we once delivered basic telephone services along the top wire of a barbed wire fence.

We have seen significant changes in our industry from the days when a "trouble ticket" consisted of determining who was moving cows that day and forgot to reconnect the jumper at the gate, and the largest "privacy concern" was that which was inherent with making a call on a party line.

What hasn't changed in our company's 71 years of existence, is our customers' requirements for privacy and security. Because of this, we have adopted practices designed to maintain the privacy of our customer's data. We do not sell customer data, and we do not collect and use customer data for the purposes of advertising or "click revenue."

We have chosen to not collect and monetize this information as a competitive differentiator, and by choosing to not collect this information, we believe we have established trust in our interactions with our customers. We have also observed general trends in online services to suggest that the market is responding to customers desire for increased protections with regards to their data, and it is our position that any legislation considered by this committee should not limit the capability of a service provider to differentiate on the basis of privacy protection practices.

Because we already do not collect and monetize customer information, we do not anticipate online privacy legislation to be overly burdensome so long as it meets certain criteria:

First, there must be consistent application of privacy protections. Legislation should establish consistent privacy protections that are technology neutral and apply uniformly to companies that collect, use, or share consumers' online personal data.

Second, we believe the pathway to success is built upon a Federal privacy framework that preempts state privacy laws. We provide services in multiple states, and having to manage a patchwork of state privacy laws will not only create an environment of uneven protections, but would create administrative burdens on small business.

Third, there must be a single Federal agency identified with the responsibility to enforce the national privacy framework. Failure to do so would result in inconsistent requirements, uneven protections, and competing priorities. We believe the Federal Trade Commission should have exclusive authority to enforce privacy protection laws at the Federal level, with State Attorneys General having the authority to enforce the new Federal law. This will allow for consistency in privacy legislation across all industries and companies as well as provide a framework for new businesses and industries to operate within. As a rural Internet service provider, we would add that the FCC should expressly be precluded from having authority to enforce privacy protection laws. Failure to prohibit the FCC from enforcing privacy protection requirements would endanger the deregulated status of Internet services.

Fourth, legislation should require companies to have a privacy policy that gives users clear and comprehensible information about the categories of data that are being collected, how consumer data is used, and the types of third parties with whom data may be shared. This type of transparency would enable consumers to make informed decision about the types of services they receive, the businesses with whom they engage, and the data privacy tolerances they are willing to accept in order to receive such services.

Fifth, legislation should not prohibit consumer-friendly incentives tied to privacy choices. Legislation should not interfere with business and consumer relationships that are based on mutually understood privacy protection tolerances. If a consumer is willing to release data in order to receive services, it should be the consumer's right to do so, and the business should be allowed to provide such services. Similarly, the market should be allowed to present data privacy alternatives as competitive differentiation so long as data privacy protection practices are clearly identified and accepted by the consumer.

Sixth, legislation should require companies to take reasonable steps to protect consumer data without prescribing a checklist of regulatory requirements.

Seventh, legislation should establish a consistent national framework and preempt the existing patchwork of state requirements on data security and breach notification. The existing environment causes consumer confusion and needless cost and complexity for companies.

Designing legislation that addresses these seven considerations would be most effective at balancing the privacy protection allowances we as consumers are willing to agree to, while at the same time, creating a business environment that can allow online services to grow and thrive in our digital economy.

Senator MORAN. We're glad to have you. Thank you very much. Ms. Dosanjh.

STATEMENT OF NINA DOSANJH, VICE CHAIR, TECHNOLOGY POLICY COMMITTEE, NATIONAL ASSOCIATION OF REALTORS

Ms. DOSANJH. Chairman Moran, Ranking Member Blumenthal, and Members of the Subcommittee, my name is Nina Dosanjh.

I want to thank you all for the opportunity to speak before the committee today. I'm a realtor, and the Director of Strategic Alliances and Technology with Vanguard Properties in San Francisco, California. I also serve as the 2019 Vice Chair of the NAR's Federal Technology Policy Committee.

I'm here today to testify on behalf of the 1.3 million members of the National Association of Realtors. Specifically, I plan to speak from the perspective of the small businesses and independent contractors that make up the vast majority of our membership.

NAR is the Nation's largest trade association. Its members, America's realtors, are involved in all aspects of both residential and commercial real estate industries.

In my role with Vanguard Properties, I'm responsible for analyzing existing partnerships, identifying new alliances that can benefit the brokerage, its agents, and the consumer.

Vanguard Properties, with roughly 400 agents, is somewhat unique in its size and the job of searching for and suggesting improvements to operational systems and technology products can be a never-ending responsibility. However, this position has also given me a unique perspective into the impact of potential privacy legislation on small realtor businesses.

Realtors have no higher priority than the relationships with their clients and the protection of their clients' best interests. Central to this relationship is an assurance that the protection of our clients' sensitive personal information.

The realtor Code of Ethics and Standards of Practice explicitly acknowledges a realtor's obligation to preserve the confidentiality of our clients' data. Additionally, NAR provides members with extensive resources and training opportunities regarding data privacy and security, emphasizing best practices for safeguarding the sensitive information we come across every day as realtors.

Real estate brokerages, like many main street businesses, rely on data to enhance revenue and drive efficiency, whether by better understanding the needs of existing customers, reaching out to new clients, or by gleaning information from existing data to drive future business decisions.

However, as the majority of realtors operate small business entities, most of us do not have the resources to employ full-time IT, legal, or security staff. Instead, we rely on off-the-shelf solutions and contractor relationships. Still maintaining the trust of our clients by protecting sensitive consumer data is paramount to the longevity and success of every realtor.

As Congress eyes legislation that can protect consumers, businesses, and our economy as a whole, NAR sees a tremendous opportunity for collaboration with this committee and with your colleagues in the House.

NAR supports six key principles in Federal privacy legislation with the aim to establish a uniform nationwide and consumer-centered data privacy law.

Namely, we believe any successful legislation must establish uniform standards for businesses and equal protection for consumers, include direct statutory obligations for all service providers handling consumer data, focus on transparency and customer choice, emphasis accountability for each business' respective actions, establish a uniform nationwide standard and enforcement for data privacy, and, finally, any such legislation must include reasonable FTC enforcement authority.

These NAR priorities are outlined in-depth in the official testimony submitted to this committee, and I'm happy to discuss further should the opportunity arise during this hearing.

In addition, states like my home of California, are moving forward to address privacy on their own. The California Consumer Privacy Act or CCPA merits the Committee's attention so that new Federal legislation does not duplicate some of the unintended consequences.

Generally, the Act is overbroad and in a number of areas including the definition of personal information and sale of said information. Specifically, I'd like to address the small business exemption. One portion of that exemption deals with interacting with 50,000 consumers or devices.

Keep in mind consumers use multiple devices to access our services. You could easily account for a home computer, a tablet, a work computer, a mobile phone. Just 137 interactions could exceed the 50,000 threshold.

In conclusion, on behalf of NAR, I would like to thank you for the opportunity to testify today. We urge you to consider these key principles as you develop Federal privacy legislation that protects consumers in a nationwide uniform consistent way without imposing undue burdens on small business members.

America's realtors look forward to working with this committee toward these goals during the 116th Congress.

[The prepared statement of Ms. Dosanjh follows:]

PREPARED STATEMENT OF NINA DOSANJH, REALTOR,
NATIONAL ASSOCIATION OF REALTORS®

INTRODUCTION

Chairman Moran, Ranking Member Blumenthal, and members of the subcommittee; my name is Nina Dosanjh. I am a REALTOR® and the Director of Strategic Alliances and Technology with Vanguard Properties in San Francisco, California. I serve as the 2019 Vice Chair of the National Association of REALTORS® (NAR) Federal Technology Policy Committee. I am here today to testify on behalf of the 1.3 million members of the National Association of REALTORS®

In my role at Vanguard, in addition to being an active real estate agent, I am responsible for analyzing existing partnerships and identifying new alliances to benefit the brokerage, its agents, and the consumer. I am responsible for researching and suggesting improvements to operational systems and technology products for the firm's agents. Vanguard Properties operates twelve offices in the San Francisco bay area with nearly 400 agents. While my brokerage is larger than the average REALTOR® business, my leadership role at NAR and engagement with fellow real estate professionals enables me to be very familiar with the impact of potential privacy legislation on small REALTOR® businesses.

REALTORS® SUPPORT CONSUMER PRIVACY

REALTORS® have no higher priority than their relationships with their clients and the protection of their clients' best interests. As a result, REALTORS® have a long history of supporting efforts to protect consumers' sensitive personal information. The REALTOR® Code of Ethics and Standards of Practice explicitly acknowledge a REALTOR's® obligation to preserve the confidentiality of personal information provided by clients in the course of any agency or non-agency relationship—both during and after the termination of these business relationships. Protection of client personal information is an important part of the trusted relationship our members enjoy with their clients and that clients expect throughout their real estate sales transaction.

NAR provides extensive resources and training opportunities to members on data privacy and security, stressing the importance of safely collecting and retaining information from clients and safeguarding their own businesses' sensitive information. NAR provides our members with online training, videos and toolkits all in an effort to help our members make privacy and data security a fundamental part of their business.

REALTORS®, like many main street businesses, rely on data to enhance revenue and drive efficiency, whether by better understanding the needs of existing customers, reaching new ones, or obtaining valuable insights to guide a wide array of business decisions. For example, REALTORS® may use consumer data to allow them to advise their selling clients on how to price their home and how many potential buyers will be interested at different price points. It can also be used to give buyers a better sense of what types of properties competing home buyers are looking at, as well as their buying ability. In sum, REALTORS® use the consumer data they collect to improve their clients experience in a way that consumers can understand and expect. Our members are not in the business of selling consumer data to third parties.

THE MAJORITY OF REALTORS® OPERATE SMALL BUSINESSES

Real estate firms vary widely in size, but the overwhelming majority is composed of very small entities. NAR's most recent surveys indicate that more than half of all residential real estate firms have less than twenty-five agents, and the typical sales agent is affiliated with an independent firm with only one office. As a result, these businesses lack the staff that a larger corporation has to dedicate to regulatory compliance.

Most real agents affiliated with residential real estate firms in the U.S. are independent contractors. In fact, 9 out of 10 NAR members are independent contractors. Any new data privacy requirements will impact the individual real estate agent who is a legal business entity separate from the real estate company with which they are affiliated. As independent contractors and small businesses, real estate profes-

sionals and firms lack teams of compliance personnel necessary to keep pace with complicated and potentially burdensome regulations. Given these characteristics of the real estate industry, NAR's top priority for any new Federal privacy law is ensuring that Congress craft realistic compliance requirements for small businesses and independent contractors.

KEY PRINCIPLES FOR FEDERAL PRIVACY LEGISLATION

Considering that the protection of consumer data privacy is a priority issue for Congress, and should be for all businesses and consumers across the nation, NAR supports six key principles in Federal privacy legislation with the aim to establish a uniform, nationwide and consumer-centric data privacy law:

Establish Uniform Standards for Businesses and Equal Protection for Consumers

Federal law should provide consumer data with uniform legal protections across all industries. Any Federal data privacy legislation should apply requirements to all industries that handle personal data and not exempt certain sectors of the economy from providing consumer data protection. The level of protection for data should not depend on arbitrary distinctions between industries, such as whether a business directly collected data from a consumer or obtained it in a business-to-business transaction. Businesses that obtain consumer information indirectly should have the same obligations and responsibilities to protect that information as the businesses that obtain consumer information directly.

Direct Statutory Obligations for All Service Providers Handling Consumer Data

Effective consumer protection regulations cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. For example, small businesses and independent contractors may lack experienced personnel, legal expertise, bargaining power or business contract sophistication to negotiate terms to require larger businesses to adequately protect the smaller business's customer data when it is in the larger business's possession. Such data service providers, particularly those offering transmission, storage, analytical processing or other consumer data services for thousands of small businesses, need direct statutory obligations to ensure they comply with relevant laws to govern customer information.

Small businesses and independent contractors, such as those operating in the real estate industry are often in substantially the same position as an individual consumer when negotiating a contract with a large service provider. Ultimately, we are left with only two choices use the service under their standard terms or go without such services, directly harming the business and its clients. Expecting small businesses to effectively negotiate contract terms surrounding privacy and data security on their own against large corporations with extensive legal departments is simply not a viable option.

Transparency and Customer Choice

Consumers deserve to know what categories of personal data that businesses collect and how that data is generally used by them. These policies should be clearly disclosed in company privacy policies and readily accessible to consumers looking to learn how their data is collected and used by the business providing the goods or services. Federal data privacy law should provide the regulatory flexibility necessary to ensure that transparency in privacy policies is provided to consumers without unnecessarily burdening businesses with requirements to seek consumer consent when they are continuing to use data based on reasonable consumer expectations.

Accountability for Business's Own Actions

Privacy legislation should not include terms that could potentially expose businesses to liability for the actions or non-compliance of a business partner. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability if partner businesses do not fulfill their own obligations under the law.

Uniform Nationwide Standard and Enforcement for Data Privacy

Congress should create a sensible, uniform Federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws effectively setting an alternative set of nationwide rules is necessary to achieve the important, national public policy

goal of uniformity while at the same time providing businesses operating in multiple states the confidence of consistency for their consumer transactions. Consumers will likewise be confident that their data is protected regardless of where they live or travel.

Reasonable FTC Enforcement Authority

The Federal Trade Commission (FTC) should have the appropriate authority to enforce comprehensive privacy regulations. NAR appreciates that the FTC employs a scalable reasonableness approach that determines the appropriateness of business practices in light of the size of the business and the sensitive nature of the data they process under Section 5 of the FTC Act. Any future privacy legislation should ensure that the FTC continues to employ flexibility in their implementation of reasonable privacy standards that will permit the Commission to enforce such regulations fairly and equitably to ensure businesses' compliance with them and to promote robust consumer protection.

Concerns with the California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) is a sweeping privacy law that will provide consumers with a number of new rights regarding their personal information but hamstring businesses seeking to ensure compliance. It is important to note that the impetus behind CCPA was the concern over the use of consumer data by internet, technology and media companies, but the breadth of the law as currently written is likely to sweep in many small businesses that were never considered to pose a threat to consumer privacy. As a result, the CCPA raises significant questions and concerns for REALTOR® businesses that we believe merit the Committee's attention so that any new Federal legislation does not duplicate the unintended consequences brought about under CCPA.

Small Business Exemption

The CCPA attempts to exempt small businesses from its application. It limits application to those businesses that meet one of three criteria 1) has gross annual revenues of more than $25 million, or 2) derives half of its revenue from the sale of consumer data, or 3) buys, sells, shares or receives for its commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices. The third criteria could sweep in small REALTOR® businesses and require them to comply with all of the provisions of the CCPA.

For example, if a consumer visits a REALTOR® website using a cellphone, a home PC and a work PC while searching for a home, which is a very common scenario during the homebuying process, then that business would have collected the personal information of one consumer from three devices. Under criteria three above, it has been calculated that the collection threshold of 50,000 consumers/households/devices equates to only to 137 visits to a website on a daily basis. This can cumulatively be met by a small number of individuals. Thus, any business operating on the Internet today can easily meet this 50,000 threshold regardless of the size or sophistication of that business.

This points out that Congress must carefully consider small business thresholds and narrowly tailor covered entity definitions in any new privacy legislation to both the size and scope of the businesses as well as the sensitive nature of data collected. Mere records thresholds are inadequate.

Impact of Right of Deletion on Multiple Listing Services (MLSs)

The Multiple Listing Service (MLS) serves as the real estate industry's internal highway, transporting data between brokers and agents. MLSs organize property listing information in a common database resulting in lower search costs, greater exposure of inventory to potential buyers, and easy market entry for new brokers large or small to compete. As a result, the MLS is critical to the home buying and selling process. Questions raised by how the CCPA will be enforced have important implications for MLS businesses. The CCPA grants consumers a right to request deletion of their personal information from businesses covered by the Act. Given the very broad definition of personal information and questions surrounding the "publicly available information" exemption, there is a possibility the CCPA, would provide a consumer the right to request the deletion of the sale price of their home from the MLS. This would result in a dramatic threat to the ongoing operation of the MLS as the comprehensive source for real estate listing data in a market area. The fallout from this loss of data would have far reaching implications beyond just REALTORS® and the MLS, as its role in determining valuation is relied upon by lenders and others in the greater real estate market and housing sphere.

Broad Definitions

The Definition of "Personal Information" is extremely broad. It covers information that "relates to, describes, [or] is capable of being associated with, or could reasonably be linked. . .with a particular household." This could be the case where the same IP address or delivery address is linked to multiple online accounts, creating difficulty responding to individual rights requests from one member of a household but not others. Thus, clarity and precision in the definition of personal information in any Federal privacy legislation is critical for REALTORS® and other businesses to build effective privacy compliance programs.

The CCPA defines a "sale" of personal information" in a manner that captures any arrangement in which a business not only sells but "rent[s]" or "mak[es] available" personal information "for monetary or other valuable consideration." The breadth of this definition captures many types of data-sharing arrangements that are necessary in today's business environment and are not viewed by consumers as a "sale" of data. For example, REALTORs® may share data with vendors to help market a client's home or to determine a competitive sales price. Congress should therefore be mindful of the importance of seamless data flows among business partners in order to deliver the efficient experiences our consumers demand from you.

Conclusion

On behalf of NAR, I thank you for the opportunity to testify today. We urge you to consider these key principles and considerations as you develop Federal privacy legislation. We especially thank you for considering the impact of such legislation on small businesses. NAR wants to ensure that any Federal legislation on data privacy protects consumers in a nationwide, uniform and consistent way and in a manner that will not impose undue burdens on our small business members. We look forward to working with you in a constructive way during the 116th Congress.

Senator MORAN. Thank you very much.

Mr. Brookman.

STATEMENT OF JUSTIN BROOKMAN, DIRECTOR, PRIVACY AND TECHNOLOGY POLICY FOR CONSUMER REPORTS

Mr. BROOKMAN. Good afternoon, Chairman Moran, Ranking Member Blumenthal.

Thank you very much for holding this series of hearings on the important and timely topic of personal privacy.

I'm here today on behalf of Consumer Reports. We're the world's largest independent testing organization. We rate thousands of products and services each year on behalf of our six million members, including evaluations of companies' privacy and security practices.

And in thinking today about how privacy legislation should apply to small businesses, it's important to consider the types of behavior we're really trying to change.

For the most part, it's the big tech companies, like Facebook and Google and Internet service providers, who have the ability to track what we do around the web and other mobile apps and increasingly in the physical world, and the data brokers, like Cambridge Analytica, whose business it is to traffic in personal information.

These are the types of companies that are the primary or should be the primary target of privacy legislation, big tech giants with the ability to comprehensively monitor our lives and niche data brokers whose business is the harvesting and selling of personal data, and I know it's become a popular talking point in D.C. that the privacy law like Europe's GDPR actually helps big American companies.

I think this is somewhat belied by the fact that those companies have traditionally aggressively lobbied against these types of bills and we're just starting to see enforcement under GDPR and pre-

dictably they're against it, these types of companies with the most invasive practices.

The French authorities levied a 50 million Euro fine against Google earlier this year. Just yesterday, a collective action was certified against Facebook in Vienna. I would argue that neither of these companies are in compliance with GDPR today and they will and should continue to feel the brunt of GDPR enforcement actions.

Now, yes, privacy law can be written badly to illegitimately favor big companies and we are seeing some concrete efforts to do that. A number of companies are pushing bills that tie privacy rights to subjective and labor-intensive risk assessments or interest balancing.

So before I have the right to tell someone to not sell my data or not to get access to it, the company does a risk assessment and decides on their own if there's a privacy risk to me and even if there is, maybe their own interests might outweigh mine.

Microsoft is pushing a bill like this in Washington State right now and Intel has published a model bill based on these ideas.

These types of bills are bad for both consumers and small businesses. They don't provide clarity or certainty for anyone. They give far too much power and discretion to the companies who can afford to hire a team of lawyers to conduct and document these types of analyses.

Instead, privacy laws should be written clearly and simply with predictable and easy-to-apply rules. Collect just the data you need, don't sell data about your customers, get rid of outdated data, use reasonable security to protect that data, and the privacy law should also explicitly carve out some limited secondary uses of data, such as Internet analytics, fraud prevention, first party marketing, so companies know what's allowed under the law, and so they don't subject customers to constant unwanted and unnecessary prompts for consent and for practices no one would object to.

There are some other ways privacy law can be crafted to specifically accommodate the concerns of small business. Thresholds have been mentioned. I think it's certainly reasonable to waive some obligations of the privacy law based on the size of the company or how much data they have and the nature of the business. So maybe access and deletion requirements or certain disclosure obligations shouldn't apply to smaller businesses but not everything. Still like a prohibition on selling data and a need to use reasonable security should always apply.

For online tracking, a law could put the compliance obligations not on the first party websites that many small businesses put up, but on the third party tracking companies that make up ad tech ecosystems.

So for a bunch of years, I worked on Do Not Track, which is the idea that you use the toggle setting in your web browser and you would tell everyone around the web you didn't want to be tracked.

And one of the most appealing things about Do Not Track is it didn't require the website to do anything. The obligation was on the ad tech tracking companies who received the signal to curtail their data practices.

In 2012, industry agreed to honor Do Not Track settings but once the regulatory attention died down, we had the Snowden allega-

tions, people were more concerned about government privacy, industry backed out of their commitment. So self-regulation failed, but a privacy law could make tracking companies honor those signals and again without first party small publishers having to do anything to comply with the law.

And, finally, quickly, data portability and interoperability are important concepts that promote both privacy and competition. They empower individuals by giving them control of their data. They also promote market choice by helping smaller companies compete with bigger ones.

Right now, the giant platforms have the ability to lock you into their systems. The portability and interoperability would force them to let smaller players compete.

So those are a few ideas about how legislation could be crafted to put the responsibilities with the right types of companies, the ones whose practices are the ones we're really concerned about.

Thank you very much for inviting me here today, and I look forward to you all's questions.

[The prepared statement of Mr. Brookman follows:]

PREPARED STATEMENT OF JUSTIN BROOKMAN, DIRECTOR, PRIVACY AND TECHNOLOGY POLICY, CONSUMER REPORTS

On behalf of Consumer Reports, I want to sincerely thank you for the opportunity to testify here today. We appreciate the leadership of Chairman Moran and Ranking Member Blumenthal not only for holding this important hearing, but also for working in a constructive, bipartisan fashion to develop smart and effective comprehensive privacy legislation for American consumers.

Consumer Reports is an independent, nonprofit organization that works side by side with consumers to create a fairer, safer, and healthier world. Consumer Reports has more than 6 million members and has been protecting consumers since 1936. We evaluate approximately 2,800 products and services each year, including testing for privacy and information security.

Comprehensive Privacy Legislation is Long Overdue in the United States

As an initial matter, it is important to keep in mind the fundamental reason we are debating this issue: the United States lacks any sort of comprehensive framework to protect personal privacy. The Federal Trade Commission has brought a number of important privacy and security cases over the past twenty years under its general purpose consumer protection authority, but its legal authority and resources are extremely limited. The considerable majority of its privacy cases have been under its *deception* authority, meaning the company had to affirmatively mislead consumers about their privacy practices. As a result, privacy policies tend to be extremely expansive and vague, providing very little in the way of meaningful information. Current law imposes few other checks on the collection and dissemintation of our personal information.

As a result of this lawless environment, consumers understandably feel they have lost all control or agency over their data.[1] Facebook and Google track what users do on the majority of sites around the web and across our different devices,[2] in other

[1] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns,* Pew Research Ctr. (Mar. 27, 2018), *https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/* (noting 91 percent "agree" or "strongly agree" that they have lost control over how their personal information is collected or used).

[2] Justin Brookman *et al., Cross-Device Tracking: Measurement and Disclosures,* Privacy Enhancing Technologies Symposium (2017), *https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.*

mobile apps,[3] and increasingly in the physical world.[4] The Weather Channel app collects personal geolocation to show you the weather where you are, and then sells that information to data brokers and hedge funds.[5] And cell carriers have been caught giving location information to various faceless middlemen, creating a virtual black market for in sensitive personal data.[6] And companies' technological ability to surveil every aspect of our lives will only increase. Policy is the only way to provide consumers with the reasonable zone of privacy they deserve.

In response to this environment, lawmakers are finally acting. Last year, California passed the California Consumer Privacy Act (the "CCPA")[7]—the first comprehensive privacy law in the United States. While key improvements are needed, the law has four basic requirements: better transparency, a right to access your information, a right to delete unneeded information, and a right to opt out of the sale of personal data. Other states—including New York,[8] Massachusetts,[9] Nevada,[10] and Washington[11]—are considering their own legislative solutions. Although Congress has passed narrowly targeted bills over the years, it has struggled to advance broader privacy legislation going back to Senator Fritz Hollings' Online Privacy Protection Act at the beginning of this century.[12] Today, however, it seems that there is relatively universal acknowledgement that *some* new legislation is needed to safeguard personal privacy, and Consumer Reports commends the Senators for their close attention to this issue.

Privacy Legislation is About Reining in Big Tech Companies and Data Brokers—Not Small Businesses

In considering how to craft privacy legislation and its application to small businesses, it is worth keeping in mind that the primary motivation behind privacy law is to combat the excesses of big Internet companies and a small number of niche companies whose primary business is trafficking in personal data.[13] The core principles and values motivating new privacy law—limiting data collection and sharing to what it reasonably necessary to deliver goods and services to consumers—shouldn't affect the core operations of the vast majority of small businesses. Notably, the examples given above about privacy violations do not involve small businesses. The ordinary collection and use of first-party data is generally permitted by most legislative frameworks; small businesses that use this information for marketing already have to comply with the reasonable requirements imposed by laws such as CAN–SPAM [14] and the TCPA.[15]

Arguably the most important element of privacy legislation is a prohibition on selling information about your customers to third-party data brokers (and for laws such as CCPA, this prohibition only applies when a consumer affirmatively opts out). However, it should be hoped that rules limiting—or at least giving consumers rights over—this behavior would not be controversial, as such sales are inconsistent with reasonable consumer expectations and constitute a violation of trust between these businesses and their customers. Yes, some small businesses—such as Cambridge Analytica and other companies who business model is predicated on accessing and selling third-party data—will be substantially affected by new privacy law:

---

[3] Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.,* Wall St. J., (Feb. 22, 2019), *https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.*

[4] Mark Bergen & Jennifer Surane, *Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales,* Bloomberg (Aug. 30, 2018), *https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.*

[5] Jennifer Valentino-DeVries *et al., 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.*

[6] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone,* Motherboard (Jan. 8, 2019), *https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-mic robilt-zumigo-tmobile.*

[7] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.198(a) (2018), *http://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB1121.*

[8] S. 224 (2019).

[9] S. 341 (2019).

[10] S.B. 220 (2019).

[11] S.B. 5376 (2019).

[12] *Senate Eyes Net Privacy,* CNN (May 23, 2000), *https://money.cnn.com/2000/05/23/technology/ftc* privacy/.

[13] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—and Won,* N.Y. Times (Aug. 14, 2018), *https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html?login=e-mail&auth=login-e-mail.*

[14] 15 U.S.C. § 7701.

[15] 47 U.S.C. § 227.

as they should be. But for most companies, privacy law should not affect their primary business model.

Privacy Law Isn't a Secret Plot to Help Google and Facebook

One curious talking point that has been aggressively pushed in DC in recent months is that privacy law actually helps companies like Facebook and Google who have more resources to develop privacy compliance regimes. The fact that this line is being pushed by groups that are funded by Google and Facebook[16]—and sometimes even those companies themselves[17]—calls into question how good faith this criticism is. In any event, given the consistency with which the attack is repeated, it is worth analyzing the validity of the argument.

First, the notion that privacy protections will entrench Google and Facebook is belied by the fact that Google and Facebook have consistently lobbied aggressively against nearly all proposed privacy legislation in both the United States and Europe.[18] Critics levied similar arguments that adoption of a Do Not Track system to make opting out of online data collection easier would favor those companies.[19] Again, however, both fought hard to stop industry adherence to that standard. And as a result, Google and Facebook (and the vast majority of the ad tech industry) ignore users' Do Not Track instructions on the web to this day.[20]

Certainly, if a company's business model is predicated *entirely* on bad privacy practices, then privacy legislation will especially impact them, and will probably disadvantage them more compared to companies like Google and Facebook—but that of course is their own fault. Both Google and Facebook have problematic practices that need to be addressed by privacy rules, but both also have core products that can be monetized effectively without collecting extraneous information and compromising user privacy. However, because those companies' business models are also heavily reliant on the use of personal information, privacy law does impact them directly—and considerably more than most companies. The Federal Trade Commission has already brought actions against both companies for privacy violations, though due to weaknesses in the law and the limitations in its own authority, its actions have not sufficiently deterred their abuses.

Finally, it is premature to judge the effect of Europe's Generan Data Protection Regulation ("GDPR")—and certainly CCPA which has yet to go into effect—on big Internet companies. As privacy advocates have extensively documented,[21] both com-

---

[16] *See, e.g.,* Letter from TechFreedom to the Honorable Charles "Chuck" Grassley *et al.* re April 10 Senate Hearing "Facebook, Social Media Privacy and the Use and Abuse of Data," & April 11 House Hearing "Facebook: Transparency and Use of Consumer Data," (Apr. 10, 2018), *http://docs.techfreedom.org/TechFreedom_Congressional_Letter-Facebook_hearing_4-10–18.pdf* (noting "Facebook has been one of many supporters of TechFreedom's work"); Testimony of Roslyn Layton before the House Subcommittee on Consumer Protection and Commerce, How the U.S. Can Leapfrog the EU—The Role of Technology and Education in Online Privacy, (Feb. 26, 2019), *https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Roslyn%20Layton%20Testimony%20Feb%2026%202019.pdf;* Transparency, Google, *https://www.google.com/publicpolicy/transparency.html* (disclosing funding for TechFreedom and the American Enterprise Institute).

[17] Sheera Frenkel *et al., Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis,* N.Y. Times (Nov. 14, 2018), *https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html* ("While Facebook had publicly declared itself ready for new Federal regulations, Ms. [Sheryl] Sandberg privately contended that the social network was already adopting the best reforms and policies available. Heavy-handed regulation, she warned, would only disadvantage smaller competitors."); Sam Schechner & Nick Kostov, *Google and Facebook Likely to Benefit From Europe's Privacy Crackdown,* Wall St. J. (Apr. 23, 2018), *https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324,* ("CEO Mark Zuckerberg recently told the U.S. Congress: 'A lot of times regulation by definition puts in place rules that a company that is larger, that has resources like ours, can easily comply with but that might be more difficult for a smaller startup.'").

[18] Carole Cadwalladr and Duncan Campbell, *Revealed: Facebook's Global Lobbying Against Data Privacy Laws,* The Guardian (Mar. 2, 2019), *https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment;* Taryn Luna, *Facebook, Google Spending Big Bucks to Fight Calfornia Data Privacy Measure,* Sac. Bee (Mar 23, 2018), *https://www.sacbee.com/news/politics-government/capitol-alert/article206394929.html.*

[19] Max Ochoa, *Why We Oppose Do Not Track and How to Fix It,* AdAge (Jul 25, 2014), *https://adage.com/article/guest-columnists/oppose-track-fix/294319/.*

[20] Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything,* Gizmodo (Oct. 15, 2018), *https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.*

[21] Norwegian Consumer Council, *Deceived by Design,* (Jun. 27, 2018), *https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018–06–27-deceived-by-design-final.pdf;* NOYB, *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and*

Continued

panies are currently in substantial violation of GDPR's provisions; it remains to be seen whether European Data Protection Authorities will enforce GDPR after a spotty enforcement record under previous privacy regimes. However, earlier this year, the French DPA levied a €50 million fine against Google for failure to comply with GDPR[22]—and just yesterday, the Vienna Higher regional court issued a decision allowing a civil suit under GDPR to proceed against Facebook.[23] So it may well be the case that GDPR will finally start to curb the worst abuses of giant Internet companies—at least in Europe.

*But, Privacy Law **Can** Be Written Badly to Illegitimately Help Big Companies*

Certainly, privacy law can be written in ways that do unfairly advantage large incumbent companies. For example, several big companies are aggressively pushing bills that predicate various privacy rights and obligations on subjective and labor-intensive *risk assessments* or *interest-balancing* that weaken consumer protections and disadvantage smaller companies without the resources to pay lawyers to conduct and document such analyses. Microsoft is pushing such a bill in Washington State (consumer advocates are universally opposed),[24] and Intel has promoted model legislation that protects consumers only when companies unilaterally determine that data processing poses a "significant" and "disproportionate" privacy risk.[25]

These types of bills fail to provide needed clarity to both business and consumers, and give far too much power and discretion to companies who can hire the best lawyers to internally justify the privacy protections to decide to offer. This concept of predicating privacy protections on risk assessments is not reflected in existing privacy statutes today—for example, the Wiretap Act[26] or Video Privacy Protection Act[27] don't ask companies to conduct risk impact assessments before privacy rights apply. Laws that pair high levels of process with weak substantive provisions are the worst of both worlds for consumers, driving up prices, and advantaging bigger, established companies over potential startup competitors.[28]

Instead, privacy laws should be written simply, with clear, easy-to-understand and -apply *per se* obligations: Collect only the data you reasonably need. Don't sell data about your customers. Get rid of outdated data. Use reasonable security to safeguard data. On the other hand, privacy law should also explicitly carve out some limited first-party secondary uses of personal information—such as for internal analytics and marketing—so that companies know what is authorized by the law, and so they don't need to subject their customers to unwanted and unnecessary user prompts for consent to engage in unobjectionable practices.

Further, there is legitimate concern that large companies' outsize lobbying power and access to policymakers will lead to bad policy outcomes. During the last bout of significant interest in privacy legislation at the beginning of this decade, big Internet companies were able to insert loopholes that weakened protections and safeguarded their own interests. Facebook, for example, infamously got a "Facebook exception" added to a bill proposed by Senators Kerry and McCain bill that would have shielded their most controversial data collection practices from the scope of the bill's protections.[29] And Google notoriously had a very cozy relationship with the Obama administration and as a result had an inappropriately large role in the de-

---

Facebook, (May 25, 2018), *https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.*

[22] Jon Porter, *Google Fined €50 Million for GDPR Violation in France,* TheVerge, (Jan. 21, 2019), *https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil.*

[23] Press Release, *Defeat for Facebook: Vienna Court admits Model GDPR Lawsuit,* NOYB, (Mar. 25, 2019), *http://schre.ms/wp-content/uploads/2019/03/PA_OLG_en.pdf.*

[24] Letter of Consumer Reports *et al.* to Washington Senate Ways and Means Committee re: SB 5376 (Protecting Consumer Data)—OPPOSE, (Feb. 21, 2019), *https://advocacy.consumerreports.org/wp-content/uploads/2019/02/SB-5376-Privacy-Coalition-Letter-Oppose.pdf.*

[25] Legislation, Intel (last updated Jan. 28, 2019), *https://usprivacybill.intel.com/legislation/*.

[26] 18 U.S. Code § 2511.

[27] 18 U.S.C. § 2710.

[28] Risk assessments may be appropriate for some small subset of processing activities like the use of artificial intelligence that could have substantial and discriminatory effects on consumers (as has been proposed by Senator Wyden in his proposed privacy legislation) but few small businesses should be affected by such a requirement. *See* Press Release, *Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy,* (Nov. 1, 2018), *https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.*

[29] Justin Brookman, *Breaking Down the Kerry-McCain Privacy Bill,* Ctr. for Dem. & Tech. (Apr. 28, 2011), *https://cdt.org/blog/breaking-down-the-kerrymccain-privacy-bill/*.

velopment of their ill-fated privacy bill.[30] However, justified concern over big companies' lobbying influence does not obviate or outweigh the very real need for privacy legislation; it does, however, suggest a need for wariness and skepticism, as well as transparency and public deliberation on the part of policymakers.

Specific Elements of Privacy Legislation that Would Appropriately Help Small Business

In developing privacy legislation, there are a number of elements that could be included to accommodate the relative lack of resources and sophistication of small businesses. Some of these elements are outlined below:

Thresholds

First, a law could waive compliance with some subset of consumer protections for companies under a certain size. The CCPA, for example, does not apply to businesses with less than $25 million in annual revenues, who do not have data on more than 50,000 individuals, and whose primary business is not the sale of personal information.[31] Of course, size and revenue alone should not necessarily be dispositive—some relatively small business can have access to a tremendous amount of personal information. For example, at the time of its acquisition by Facebook, Instagram had only thirteen employees and negligible revenues; nevertheless, it hosted the personal information of tens of millions of users.[32] Access and deletion obligations may be good candidates for exceptions for small businesses with limited personal information; also, heightened transparency obligations might only apply to larger businesses with access to greater stores of data.[33] On the other hand, some obligations—such as a prohibition on sale of customer data and a duty to use reasonable data security—should attach regardless of the size and scope of personal information possessed by a company. Nevertheless, an assessment of what is "reasonable" for any individual company may appropriately consider a company's size and available resources (as well as other factors such as the sensitivity and scope of data in its possession).

Exempting Pseudonymous Online Data from Access and Deletion Requirements

Other provisions in a thoughtful privacy law could make compliance easier for small companies. For example, while a privacy law should apply broadly to a wide range of information—including online data associated only with a cookie or IP address—exempting certain data from access requests would ease the burden of compliance, prevent illegitimate access to personal information in shared environments, and incentivize companies to maintain in less identifiable forms. While most of a law's protections would apply to device-level or household-level data (such as transparency and a prohibition on sale), those types of data could be exempted from deletion and access requirements. This is justified on policy as well as burden grounds since such data cannot reliably be authenticated, so companies could not confidently know data they possess actually pertains to a requestor. Currently, this is an issue being considered in California with regard to the CCPA, and Consumer Reports and other advocates have urged the Attorney General to promulgate rules stating that data linked only to pseudonymous identifiers (like cookies, device identifiers, households, or IP addresses) should be broadly exempt from access requests.[34]

Similarly, a privacy law could explicitly state that companies need not collect or retain additional data in order to comply with a privacy law. This too is currently a contested issue with the CCPA, as several trade associations have asserted this

---

[30] Natasha Singer, *Why a Push for Online Privacy Is Bogged Down in Washington,* N.Y. Times (Feb. 28, 2016), *https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html.*

[31] CCPA, § 1798.140(c).

[32] Victor Luckerson, *Here's Proof That Instagram Was One of the Smartest Acquisitions Ever,* Time (Apr. 19, 2016), *http://time.com/4299297/instagram-facebook-revenue/*

[33] Comments of Consumer Reports to the National Telecommunications and Information Administration re Re: Docket No. 180821780–8780–01, Request for Comment on the Administration's Approach to Consumer Privacy, (Nov. 9, 2018), pp. 6–7 *https://advocacy.consumerreports.org/wp-content/uploads/2018/11/CU-NTIA-Docket-No.-180821780-8780-01.pdf* (comments on appropriate role of transparency in privacy legislation).

[34] Comments of Consumer Reports re Rules Implementing the California Consumer Privacy Act at 4–5 (Mar. 8, 2019), *https://advocacy.consumerreports.org/wp-content/uploads/2019/03/CR-CCPA-Comments-to-CA-AG.pdf.* It might also be appropriate to exempt data that could be used for identity theft from access requirements, as the utility to consumers is marginal, and the potential abuses considerable.

is a concern with the law.[35] This was certainly not the intent of the CCPA drafters and is based on a questionable reading of the statute; still, clarifying that companies don't have an obligation to engage in more invasive tracking in order to comply with privacy legislation should be noncontroversial.

Put Compliance Obligations on Tracking Companies—Not Websites

Privacy law can also be constructed to transfer compliance obligations from small publishers to the large data broker and tracking companies who are the primary target and concern of the law. For example, in response to petitions from privacy advocates,[36] the Federal Trade Commission in 2010 proposed a "Do Not Track" system to empower users to stop—or at least substantially curtail—online behavioral tracking.[37] Major browser companies created a setting that allowed users to broadcast a Do Not Track signal as they surfed the web.

Importantly, this system did not impose any obligations on websites themselves—just on the third-party tracking companies that monitored user behavior across different sites.[38] In 2012, the major ad tech trade associations publicly committed to honoring Do Not Track settings;[39] however, within a handful of years, they had completely reneged on their promises.[40] Today, users' Do Not Track instructions are nearly universally ignored. This failure of industry to respond in good faith to users' privacy settings highlights the need for this body to advance privacy legislation. In order to achieve what Do Not Track ultimately failed to do, a privacy law could include a mandate that third-party vendors adhere to users' stated privacy preferences, while absolving website publishers from any obligations other than to pass those signals along to tracking services.

Provide for Data Portability and Interoperability to Allow Small Providers to Compete with Larger, Incumbent Players

Finally, strengthening consumer agency with regard to their own data can also promote competition and market choice. Data portability and interoperability requirements can accomplish both important policy goals by giving consumers control over their data while helping small businesses compete with big companies. While data portability allows consumers to take their data to innovative and privacy-protective new services, it can only be accomplished when the digital ecosystem is interoperable. In its report on "Unlocking Digital Competition," the United Kingdom's Digital Competition Expert Panel found that, "the development of common standards for sharing data has huge potential to improve consumer choice and boost competition."[41] Indeed, requiring interoperability protocols can facilitate competition in the face of the strong network effects that make consumers feel locked into dominant incumbents.

Conclusion

For good actors, privacy law should be straightforward to comply with: ordinary, first-party data collection and processing for fulfilling customer orders—as well as expected operational uses like analytics, fraud prevention, and even marketing—

---

[35] Wendy Davis, *ANA Presses California To Refine Privacy Law,* MediaPost (Feb. 15, 2019), *https://www.mediapost.com/publications/article/331560/ana-presses-california-to-refine-privacy-law.html* (arguing "'[t]he CCPA could have the unintended effect of forcing business to associate non-identifiable, pseudonymized device data with a specific person seeking to exercise their CCPA rights'").

[36] *Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles,* Fed. Trade Comm'n (Dec. 20, 2007), *https://www.ftc.gov/public-statements/2007/12/online-behavioral-advertising-moving-discussion-forward-possible-self.*

[37] Ira Teinowitz, *Chairman: FTC Leans Toward "Do Not Track" Registry,* Ad Age (Jul. 27, 2010), *https://adage.com/article/news/chairman-ftc-leans-track-registry/145131/.*

[38] The Do Not Track system was proposed to address the myriad deficiencies in extant industry opt-out programs, including lack of universal applicability, failure to address data collection and retention, and technological limitations. For more on the history of Do Not Track and the inadequacy of industry self-regulatory efforts, *see* Testimony of Justin Brookman Before the House Subcommittee on Digital Commerce and Consumer Protection on Understanding the Digital Advertising Ecosystem, (Jun. 14, 2018), *https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-Wstate-BrookmanJ-20180614.pdf.*

[39] Rainey Reitman, White House, Google, and Other Advertising Companies Commit to Supporting Do Not Track, Elec. Frontier Found., (Feb. 23, 2012), *https://www.eff.org/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supp orting-do-not-track.*

[40] Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything,* Gizmodo, (Oct. 15, 2018), *https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.*

[41] Jason Furman *et al., Unlocking Digital Competition—Report of the Digital Competition Expert Panel,* (Mar. 2019), *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.*

should be generally allowed, without forcing consumers through unnecessary consent dialogs and permission requests. Companies will still have some obligations—notably, not to sell customer data and to use reasonable data security—but at least the latter is already required by a growing number of state security laws as well as existing prohibitions on unfair and deceptive practices. Bigger companies should be expected to respond to access and deletion requirements, but the bulk of these requests will be directed at the Internet giants who have the power and scale to build up rich, detailed profiles about consumers. Privacy legislation is primarily designed to check the power of these dominant companies—as well as data brokers who specialize in trafficking personal data. Ultimately, a well-written privacy law should tilt the balance of power in favor of smaller companies whose business models aren't predicated upon tracking every aspect of consumers' lives.

Senator MORAN. Thank you very much for joining us. Thank you all for joining us, and I found the testimony very valuable.

Let me start with a question for Mr. Weber. Your testimony points to specific harms that come from pre-determined levels of fines authorized by the CCPA.

"Acknowledging that some privacy laws, like CCPA, currently provide minimal small business carve-outs, it is still absolutely necessary for any Federal privacy enforcement authority to consider certain metrics to ensure appropriately proportioned penalties, including the size of the business, the availability of resources, and the scope and sensitivity of the data and its data processing practices."

If first-time civil penalty authority is on the table for Federal legislation, would you agree that these factors should be taken into account? In addition to those factors, what others might need to be included?

Mr. WEBER. For the ones that are available for us to use as a metric to compare against, like the GDPR, CCPA, I mean that's a huge concern that it's kind of a first time and you're immediately fined and the guidelines represent millions of dollars or percentage of revenue, that again is a death blow to these companies, but, you know, for small businesses, again how we define that business is going to be a challenge.

I think maybe in tech, it is different than what the SBA defines as a small business in America because for a number of reasons, but, yes, I mean, there's a potential and I think a good impact where first offense taking a bit of a warning would be extremely helpful to particularly startups.

Any fine that would be distributed for, say, from the FTC would essentially make them unable to really scale from there. It'd be very hard to find investors, customers, users, and reputational risk would be at an all-time high.

Senator MORAN. Thank you.

Let me turn to the realtor. I'll call you Madam Vice Chairman. How can policymakers ensure that anyone who handles sensitive information, social security numbers, substantial amounts of consumer financial information, as I would expect a realtor to do so, is not going to share that information with unknown third parties or use it in ways that's harmful to the consumer?

Ms. DOSANJH. Sure. So realtors do not collect sensitive personal information. The data that we collect on our consumers is more just their personal contact information and maybe their preferences on the types of, you know, properties and features that they like

in the property, but we do not collect personal information. The lender usually handles that.

Senator MORAN. So you would be safe and secure from at least part of the components of any legislation that we might pass?

Ms. DOSANJH. Correct.

Senator MORAN. And that's, I guess, the point, is that you ought to be treated differently——

Ms. DOSANJH. That's right.

Senator MORAN.—than somebody who does collect that kind of information?

Ms. DOSANJH. Yes.

Senator MORAN. OK. Mr. Engstrom, in particular startup businesses, that community, would you describe for me the concerns associated with providing a private right-of-action in a Federal consumer privacy law?

Mr. ENGSTROM. Yes. Thank you for the question, Senator.

It's certainly one of the aspects of CCPA that we're most concerned about, mostly because whenever you combined a private right of action that is untethered to any actual harm suffered—in the CCPA, they have statutory damages available for any data breach, plus a sort of ambiguous liability threshold in CCPA, it's reasonable security practices—you're opening up the door for lengthy litigation and that's the real concern here because once you have a data breach and, frankly, you know, no matter what companies do, there's always the risk that something bad will happen, you know, it's a truism in this industry that it's not a question of if you'll run into a problem with security, it's when, and we want to encourage companies to do the best thing possible and implement the best security measures possible, but that's generally not a determination you can make early in a litigation.

So for most companies, any time something happens, no matter how responsible you were, the threat of statutory damages not tied to any actual harm is going to require a long litigation that's going to frankly bankrupt a company, if they win or if they lose, because there are no attorneys fees associated in CCPA.

So I think the risk of inviting litigation, that's going to drag out and drain a company's resources, is a very real threat.

Senator MORAN. What are the factors that cause your sentence, I have no doubt but what it's true that says "that there's going to be a breach, there's going to be a privacy invasion?" What's the factors in the environment that make that sentence true?

Mr. ENGSTROM. So I think any time, particularly CCPA requires, you're going to have to collect more information. So if you're a company and you have to, say, verify the identity of a user in order to comply with the deletion request, which is what CCPA envisions, you're now having to collect more information about that user in order to identify this is actually you seeking the deletion of your information.

That's a great deal of info that you're holding, valuable info. It's going to attract bad actors. You see sort of inadvertent mistakes, no matter in what good faith you're operating in. Sometimes bad stuff happens. It doesn't happen across the board but it is a very real risk when you're talking about important vast stores of information online.

Senator MORAN. That information is still valuable to other people, that there's so many people who want to obtain it that it's worth the risk, right?

Mr. ENGSTROM. Senator, absolutely. It can be and, you know, people might just want to see what you have ultimately, even if it's not valuable.

Senator MORAN. Mr. England, your company operates in at least two states, maybe more.

If every state in which you operated passed its own consumer privacy law, how complicated would compliance be? You talked about this in your testimony. Any ability to expand on that?

Mr. ENGLAND. Sure. Thank you, Senator.

You're absolutely right. We do operate in both Idaho and in Wyoming and if each of those states had their own separate privacy protection laws and legislation around how to treat that information, it would create administrative burdens for our organization because for the obvious reasons, that we'd have to staff people with expertise and knowledge and understanding around each of the frameworks within each of the locations.

It would perhaps change workflow processes within how we service those customers, and it's precisely why I listed that as one of our top three concerns about any legislation is that it would have the Federal nature that would preempt any state legislation.

Senator MORAN. Before I turn to Senator Blumenthal, let me get on the record this question of preemption because it's an important one that we're going to be trying to find a solution to.

Would your organizations and businesses that they represent support Federal legislation to preempt inconsistent state privacy laws in the interest of providing fair privacy expectations and protecting consumers? Mr. Weber?

Mr. WEBER. Yes, Senator, they would.

Senator MORAN. Mr. Engstrom?

Mr. ENGSTROM. Yes, Senator.

Mr. ENGLAND. Yes, Senator.

Ms. DOSANJH. Yes.

Mr. BROOKMAN. Inconsistent ones, sure, but the states still need to be allowed to innovate for things that are not covered by a Federal law.

Senator MORAN. OK. Senator Blumenthal.

Senator BLUMENTHAL. Thank you.

Let me ask you the same question but assume that the privacy protections are equivalent to the California law. In other words, preemption but the same protections or greater with the exception of possible—I think you mentioned it, Mr. England, or one of the panelists, that technology might create new challenges that the states would have to innovate in their statutes to address.

But let's assume for the moment it's California law, would you still favor preemption? Mr. Weber?

Mr. WEBER. I'm not absolutely familiar with the California law, to be totally honest with you. I think for our members and those that are just now diving into what that impact is going to be on them, I can——

Senator BLUMENTHAL. Well, how about GDPR?

Mr. WEBER. Again, I think there's consensus with our companies that GDPR is pretty good. There's general support of that law. There's some things that are very concerning to those companies, including the enforcement and fines that we discussed earlier.

Senator BLUMENTHAL. Well, let's assume the same enforcement and fines. You have to have a means to make it real.

Mr. WEBER. Yes. I think again the——

Senator BLUMENTHAL. In fact probably enhance fines and enforcement.

Mr. WEBER. Yes. It's hard to assume. I mean, obviously the preemption factor is the one unanimous thing that I remember companies I spoke to mentioned as very important to them.

Now comparing it to CCPA or GDPR, I don't know that I can comment on that.

Mr. ENGSTROM. Senator, thank you for the question. I would say the rights in California's law are correct. I think users should have a right to have more transparency about how their information is used. I think users should have more rights about accessing and gleaning information and they should have more rights about how companies use that.

I do think it needs to be a little more narrowly cabined to avoid some of the contradictions that are in the law and some of the problems, like I mentioned in my testimony, that would actually decrease user safety.

So I think there are things that we need to improve in the California framework but the rights themselves, I think, are laudable, important. We should adopt them and, frankly, I think there are many ways we can go farther.

For example, I think the California law doesn't really envision any user rights over the collection of information and that presents—you know, any time we're talking about user privacy, I think we have to pay attention to what companies have in the first place, not just how they're using it.

So as long as the problems with the law, some of the ambiguities, some of the contradictions are ironed out, I think the rights themselves are important and can be built upon.

Senator BLUMENTHAL. Thank you. Mr. England?

Mr. ENGLAND. Yes, thank you, Senator. In all truthfulness, I didn't really even know what GDPR or CCPA were until earlier this week and if maybe there are some strengths in that as part of my testimony, I would say that as a small business provider, it is really burdensome to try and track all of these down.

So if your question is around the particulars of the CCPA law, I don't know that I can really add much valuable comment or testimony on that.

If your question is around whether or not states laws are to be in line with Federal, then I think the preemption is perhaps the better placement there.

Ms. DOSANJH. So we do support a single Federal standard as opposed to 50 different state standards. That would be our——

Senator BLUMENTHAL. But what——

Ms. DOSANJH. In terms of GDPR.

Senator BLUMENTHAL.—happens with the California law as a floor, not a ceiling but a floor, as to what the protections should

be? You don't get to eat dessert without the meat and potatoes, right?

Ms. DOSANJH. Right.

Senator BLUMENTHAL. Preemption is the dessert.

Ms. DOSANJH. Yes.

Senator BLUMENTHAL. It's what everyone wants.

Ms. DOSANJH. So in terms of the definition in CCPA, I mean, I think we would agree to some type of revenue threshold and we would think we would want, you know, some sort of consideration for how the businesses use the data and, like I said before, realtors are not in the business of selling the data. So we would prefer one uniform standard.

Senator BLUMENTHAL. Well, not only, if I heard you correctly, in the business of selling the data but you don't collect it.

Ms. DOSANJH. Correct.

Senator BLUMENTHAL. Is that true of all your members?

Ms. DOSANJH. So in terms of the data we collect, we don't collect sensitive—so the definition of personal information, that's the kind of ambiguity in CCPA is that personal information and the sale of said information is not clearly defined.

So we think that that definition would need to be uniquely tailored.

Mr. BROOKMAN. And again the laws are inconsistent and I think preemption makes sense, but as Mr. Engstrom pointed out in California law, it has a lot of good things, a lot of things that could be strengthened, doesn't do. So the state wanted to do something to address collection. The state wanted to do something to address facial recognition right, which they thought they specifically addressed in the bill.

States like Illinois, Texas, should have the right to do that, to kind of build on new things as they develop. I love you all. You all do a great job but you tend to move fairly slowly, right, and so, you know, we've been debating privacy law since Senator Fritz Hollings, my senator, introduced a bill in nearly 2000. So the states need to be able to iterate in between.

Senator BLUMENTHAL. Thank you.

Let me take another poll, if I may, and these answers are very helpful to know what your thinking is and they're all extremely insightful and illuminating.

On enforcement raised by Mr. Weber, I'm assuming that you would all support the FTC having rulemaking authority, correct? Everybody's nodding.

Mr. BROOKMAN. Yes.

Senator BLUMENTHAL. Do you support the FTC being able to bring civil penalties for first offenses? I'm happy to entertain answers, as long as the Chairman allows me to keep going.

Mr. ENGSTROM. Senator, yes, I think we would. I mean, obviously we want to make sure they are reasonably tailored to the particular harms, but I——

Senator MORAN. You can continue as long as you want, as long as you tell me what your question was. What did you just ask?

Senator BLUMENTHAL. The question was should the FTC be able to seek civil penalties for first-time offenses?

Mr. BROOKMAN. I mean, Cambridge Analytica was the first-time offense, right, and the only—like you do bad thing—again, you can take into account it wasn't a repeat offender. You can take into account the size of the operation. You can take into account how bad it was, but I don't think everyone should get one automatic free bite of the apple like they get today under Section 5.

Senator BLUMENTHAL. So you're saying yes, there should be civil penalty?

Mr. BROOKMAN. Absolutely.

Senator BLUMENTHAL. Anyone disagree?

Ms. DOSANJH. So we would say that damage caps should be a part of that discussion.

Senator BLUMENTHAL. OK. Well, that's really the point I think that Mr. Engstrom was making. The reasonability of the—so you might opt in favor of a graduated system, first-time offense, a cap, second offense, maybe a higher cap. That's a pretty customary regime in the law.

Do you support the State Attorneys General being able to enforce the Federal law?

Mr. ENGSTROM. Senator, I think ultimately the concern we would have with State Attorneys General enforcement is if the Federal law is either too ambiguous or too flexible. If an individual Attorney General is allowed to interpret the law in a different way, you effectively create 51 different jurisdictions.

So I think as long as there is a very clear nexus between how the FTC interprets the law and how it's being enforced, those problems are mitigated.

Senator BLUMENTHAL. Other comments?

Mr. BROOKMAN. I'd say as a former Assistant State Attorneys General, I strongly support it. I mean, the FTC has, what, 50 attorneys looking at whatever trillion economy. I think they do a decent job with the resources they have. They brought four privacy and security cases last year. I mean, I think you absolutely need—and some states do really, really good things.

New York State recently bringing some tough enforcement actions and so I think absolutely need to have more sheriffs on the beat. I think, you know, make sure it's something clear they can enforce. That goes back to my point. The law should be clear and understandable in the first place.

Senator BLUMENTHAL. Well, as a former Attorneys General of the state of Connecticut, I just happen to share that view and going to your point about FTC enforcement, do you think that the FTC should be given more staff and resources to do its job?

Mr. WEBER. I would support that. This is going to be a very complicated issue for enforcement.

Mr. ENGSTROM. Yes. Absolutely. I think it does. The FTC should be properly staffed to enforce a strong Federal law.

Mr. ENGLAND. [Nods Head.]

Ms. DOSANJH. Yes, Senator, we agree.

Mr. BROOKMAN. Yes.

Senator BLUMENTHAL. And I assume you agree?

Mr. BROOKMAN. Absolutely, yes, and I was also a former employee of the Federal Trade Commission. I think they absolutely need more resources.

Senator BLUMENTHAL. I must say just in closing that I'm very concerned about data brokers. We have seen firsthand some of the impacts of the practices and abuses on the part of data brokers.

I recognize that you may have some drafting suggestions, but it seems to me that whatever law we have, the business model of data brokers is to build powerful profiles of individuals based on their consumer information.

We have investigated data brokers, the Congress has, and, quite frankly, these companies should be embarrassed as to how they often treat people. They categorize them, for example, in one instance as rural and barely making it.

Anybody have suggestions about what should be done about data brokers?

Mr. BROOKMAN. Yes. It goes back to one of the principles that talked about don't sell information about your customers. I mean that should be a basic—we talk about whether it's opt-in or opt-out or assumed—you know, just don't it.

I mean that's how they get it. They're allowed right now to sleazily secretly collect information about what we do online. They're allowed to—when you go to the grocery store, there's nothing to stop the grocery store from telling you whether you're getting Stouffer's frozen pizza or kale. There's just no visibility, transparency into that whatsoever.

So transparency would help but also if there's a clear right to say knock that off or, you know, a presumption like just don't sell your customer's data, just don't do that. I think that would actually kind of cut off the stream.

Senator BLUMENTHAL. Well, let me thank you for your answers to all these questions.

My sort of take-away from what you've said is that you endorse the basic principles of privacy. You want to avoid the costs and unintended consequences that may be more burdensome for small businesses than they would be for large, but the customers, at least your customers, are not your product as they are in the business model of Facebook and Google, and therefore your interests overall is in protecting them.

At the same time, you have to stay in business and just understanding, as Mr. England said so well, the law sometimes is a burden. We know about it in the tax area. Understanding tax law is extraordinarily challenging and small businesses are the lifeblood of our economy, creating more jobs than any other sector.

So we respect what you do and I think preemption is certainly something we will need to consider how to frame, but one of the purposes of Federal law is to prevent inconsistencies and also raise the bar.

So I think we have had a very productive session here and I want to thank you for being here.

Senator MORAN. Let me have a few follow ups. Mr. Engstrom and Mr. Brookman, both of you agree that the FTC is the place that enforcement should reside, is that true?

Mr. ENGSTROM. Yes, Senator.

Mr. BROOKMAN. They should be the primary enforcer.

Senator MORAN. The primary enforcer. I'm not meaning to exclude attorney generals in that question, state attorney generals.

And do all of—those of you who represent a business or organizations that collect data, do any of those you represent sell data?

Mr. WEBER. Yes, Senator, I'm certain there are companies in our membership that absolutely do sell data.

Senator MORAN. And that's obviously part of their business plan for making a living, right, earning a profit?

Mr. WEBER. Yes. I think for a lot of online companies, if there's not a cost to use that service, it's assumed that there is data being sold for revenue and advertisement. Yes, Senator.

Senator MORAN. And so when we talk about prohibiting the sale of data, what would that mean for your members?

Mr. WEBER. I think it's a giant concern but also it's important to ask the second question of what data is being sold. If it's not sensitive data or personal data, then, you know, could that be treated differently? That would be an important distinction for some of our member companies. We're not talking about a lot of them, though.

Senator MORAN. Others? Mr. Engstrom?

Mr. ENGSTROM. Senator, thank you for the question. At the outset, we are not a formal trade association but the companies we work with, I think clearly under the definition of sale in the California law, virtually everybody sells data because it's so broad that it would encompass a huge range of practices that don't normally fall into what we might think of as a data brokerage business.

It's about sharing information with third parties and the way it's defined in California, I think, is pretty broad.

But to your point, I think it's important to not go too far down the path of making ad-supported companies impossible to operate as an early stage company. Far too often, early stage companies don't have the kind of reputation that they would need in order to have a subscription-based service.

So if we go too far down the path of making ad models impossible to operate, you're really just going to hurt the small companies that can't shift toward a payment system.

Senator MORAN. Mr. Brookman, you're the one who caused me to raise this question.

Mr. BROOKMAN. Yes. I mean, I have no problem with showing folks ads. I like advertising.

I do object to the notion that companies have a right to track what I do all around the web in different apps and what I buy in the store where I go in order to monetize their startups. At the very least, I think there should be some sort of clear scalable opt-out rights around that. I think you could probably go farther, but to say no, we need to carve out all of that, we have an obligation to collect and share all this—and I think it is sensitive data. You know, everything I do online everywhere I go, to say there should be no autonomy over that because innovation, I think most people would disagree with that.

Senator MORAN. Let me call on the Senator from South Dakota, Senator Thune.

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

Senator THUNE. Thank you, Mr. Chairman.

Mr. Engstrom and Ms. Dosanjh, striking the right balance between ensuring consumers' data is protected and encouraging private sector investments and innovation is a key part of this discussion.

In each of your testimonies, you state that the CCPA's definition of personal information is overly broad and would cover nearly all information related to an individual user.

What would be the implications of I should say to your member companies if that definition were adopted at the Federal law?

Mr. ENGSTROM. Senator, thank you for the question. As you point out, the definition of personal information covers, I think, every conceivable piece of information about a person as it's defined in CCPA. It is anything that could possibly relate to a person. That would cover—I can't imagine what that wouldn't cover. That would cover your hair color. That would cover anything about you.

So really it depends obviously how that definition is baked into Federal law. If there are restrictions on how companies can use personal information or collect personal information, it suddenly becomes very burdensome, of course, because it's so wide-ranging.

If there's an associated deletion right, a company now has to search through its IT systems to find any possible conceivable piece of information that might theoretically relate to you, wholly independent of the harm associated with the disclosure of that information.

So it just greatly expands the scope of what companies need to do to comply with any sort of deletion or access right and it gets to a point where I'm not sure it's manageable for any company.

Senator THUNE. Ms. Dosanjh.

Ms. DOSANJH. Senator, thank you for the question.

What I would have to say in terms of personal information for realtors is we don't necessarily collect financial information. Our personal information that we collect from realtors is—I mean from consumers is, you know, their habits and what property features they want to see in the home that they're going to buy.

So we're not really in the business of selling data. So I would have to agree with Mr. Engstrom and his statement.

Senator THUNE. So legislative action on the subject of consumer privacy is taking place in several states. So just as a follow-up, do any of those states have a definition of personal information that should be considered at the Federal law?

Mr. BROOKMAN. I would say briefly, I support having an expansive definition of personal information, like CCPA's. I think it's pretty good.

I'm sympathetic to some of the concerns I heard about—and so I think certain categories, like device information and household data, should be maybe carved out from access and deletion rights, but I still think you should be able to have the right to turn off the sale of that right.

If you go to like shoes.com and say opt-out and you still see the shoes following you everywhere you go around the web or you get added to Senator Blumenthal's urban drugs category because the shoes are cheap, despite trying to take some action to stop that, but I think that that sort of information should—there should be some rights around that.

Senator THUNE. Mr. England, could you elaborate on the effects a patchwork of state privacy laws would have on your company?

Mr. ENGLAND. Yes. Thank you, Senator. Being located along the state line of Wyoming and Idaho, we serve multiple states and our network expands between each and we have customers and service technicians that service all of that area.

Our greatest concern or one of our top three greatest concerns with any sort of legislation would be to have some consistency because as a small business and as was pointed out earlier, I'm struggling just to keep up with what GDPR and CCPA even is, let alone some of the terms around it, and if we had multiple states with their own versions that we would have to be in compliance with as a small business, it becomes burdensome in terms of resources to be able to keep up with the differences between each. It may change some of our business practices, how we go about servicing the customers.

I think it's also important to point out, as a small rural Internet service provider, every dollar that we have available to us through our earnings and through our business practices, we roll back into deploying additional plant and facilities to service our customers and so for us, it's a value proposition, as well.

Obviously we want to make sure our customer information is kept safe and protected, but having unnecessarily burdensome patchwork policies in our case what actually diverts some dollars away from continued deployment of services to our customers.

Senator THUNE. And that's what I was going to ask you because the compliance costs associated with that sort of a patchwork regulatory system seems that it would draw resources away from what you might otherwise spend on broadband services to consumers in unserved areas. Is that a fair statement?

Mr. ENGLAND. Absolutely.

Senator THUNE. OK. This is for Mr. Engstrom. Apple CEO Tim Cook has advocated that data brokers register with the FTC. What are your thoughts on that proposal, and can you speak to the ways your member companies use data brokers and for what purposes?

Mr. ENGLAND. Senator, thank you for the question. I guess as an initial matter, as not a trade association, we're an advocacy organization but a formal member, so I can't speak to individual company practices on this, and I would need to dig in a little more into the proposal that Mr. Cook put forward.

I would say the key is to define what we mean by data broker. I think that's really important here. I'm concerned that in trying to get at really bad practices, you know, selling user information where there's no transparency, where users have no idea what's happening, you might be getting at core ad tech functions where, say, aggregator anonymized information is being shared for purposes of improving a site's functionality.

So without seeing the specifics of how data broker is defined in such a proposal, I would be cautious to comment on it. I do know it's incredibly important for small businesses to have access to information for purposes of running ad-supported companies which, as I mentioned earlier, for early stage companies where you don't have a user base yet, where you don't have a reputation, it's very

hard to offer a paid product. So you rely on ad-supported functionality to get off the ground.

Senator THUNE. Mr. Chairman, my time has expired. I have one other question I can submit for the record.

Mr. England, you mentioned in your testimony that the FTC should be the sole Federal agency involved in enforcing a new Federal privacy law and you may have already discussed this or have already discussed this, but I would just ask if you could elaborate on why you think that the FTC has more expertise when it comes to privacy than the FCC?

Mr. ENGLAND. So I believe in my understanding and visiting with others who are more familiar with the history of the law and the involvement of the FTC that they've got a long rich tradition of being able to enforce these types of protections and I think it's not something that the FCC would have the same capabilities and reach.

One of the reasons why is because one of my key principles that I believe the legislation should include is that it should be technology-neutral. It should apply to all industries and it has less to do with who is actually collecting the data and far more to do with what types of data is being collected and what's being done with it.

The FCC, of course, is limited to the communications industry and I think the FTC has the reach that extends far beyond into all industries that could affect—has the potential or risk of privacy concerns.

Senator THUNE. OK. All right. Thank you. Mr. Chairman, thank you. Thank you all for being here.

Senator MORAN. Thank you, Senator Thune.

I'm going to follow up with a few questions. We'll see if Senator Blumenthal has any others and then we'll conclude our hearing, unless other members return.

I'm going to talk about—this is somewhat related to what I heard when we talked about attorney generals, state attorney general enforcement, someone, maybe you, Mr. Engstrom, I don't want to put words in your mouth if it wasn't you, indicated you could end up with 51 different jurisdictions interpreting the Federal law and you end up with 51 different standards, something that is a topic of conversation about trying to avoid, something that most of the panelists here are supportive of.

So in terms of a Federal privacy—I'm sorry. In terms of a Federal consumer privacy bill, how do we get the FTC, the rulemaking authority we give them, it needs to be pretty specific, and do we do that with some kind of curbs that restrict their flexibility?

I mean, on one hand, there are so many different instances in which consumer privacy is in jeopardy. The circumstances are different. You all asked for flexibility when it comes to small or start-up. So if we have one standard, a rulemaking authority that says you can make rules in this regard, how do we provide the FTC the necessary flexibility to meet the variety of circumstances at the same time not create an opportunity for 51 different jurisdictions to interpret the law differently?

Mr. ENGSTROM. Senator, thank you for the question. I think it's an incredibly important point on this issue and really across any

technology policy issue, the need to balance certainty with flexibility to adapt to changing technological issues.

I think in this context, I would say on something like, say, the definition of sensitive information, I'd like to have as precise of a definition as possible in a Federal law but recognizing that, you know, 20 years ago, we weren't really talking about facial recognition activities as being possible. So you need to have some mechanism built into FTC rulemaking to adapt the law to take these in into account.

Another example would be in the context of, you know, reasonable security practices. Let's make sure that there are some guardrails around what we consider to be reasonable, things that are encouraged, things that are legal, and then within that framework allow the FTC to build upon that as new technologies, like differential privacy or synthetic data, start to emerge, and not sort of curb the growth of pro-privacy practices because, you know, the legislatures can't simply keep up with changing technologies.

Senator MORAN. Will the market demand greater privacy protections? We talked about opt-in, Mr. Brookman, and opt-out. What are consumers—do consumers have a sufficient level of knowledge and interest in what is happening to their information? Will companies find it necessary to compete in this business of data collection by providing greater privacy market forces that play at all in this world?

Mr. BROOKMAN. I hope so, yes. I'm at Consumer Reports and we are investing a lot of resources in trying to rate and evaluate services for just these reasons. It's really tricky as though if I'm trying to evaluate two cloud services, like what happens to my data when it goes to the cloud. I can't watch that in the lab. I have no visibility into what Google or Facebook or Amazon or whoever does with that data.

I can try to look at their privacy policies and we look at privacy policies, but, you know, you all look at the privacy policies, they're not very illuminating because primary law in this country is don't lie about privacy. Privacy policy is going to be very vague and expansive and very mushy. So it's going to be very hard to get actual information. Even when we have the time, like we have a full-time employee looking at privacy policies, they have a very difficult time in differentiating and so consumers trying to evaluate between two different apps, they're right now not equipped to do that.

We're trying to provide more information to the marketplace but again given the lack of transparency obligations even, it's even hard for people who do it full time to do it.

Senator MORAN. Anyone else on that? Mr. England?

Mr. ENGLAND. Yes, Senator, thank you. I'll add just from my personal experience that we see within our service area.

I think I can't remember the phrasing the EU used. I wouldn't say that all consumers are more aware. There are certainly a number of customers who don't know and maybe it's just because it's overwhelming to try and figure it all out and maybe it's also because they're all so suspect that all of their information is out there anyway.

But I can tell you that we have more customers who are calling and asking about privacy-related issues than perhaps we've ever

had before and so I think that the general trend among consumers in our service area is that, yes, more and more becoming aware of the issues and want to know what is being done about it.

Senator MORAN. OK. Thank you.

This is intended for any or all. How should we treat de-identified and aggregated consumer data in the definition of personal information in a Federal privacy bill?

Mr. ENGSTROM. Senator, thank you for the question. I'll jump in here.

I think it's incredibly important to have carve-outs when companies are engaging in practices that minimize security risks through de-identification, through aggregation. It's obviously a hard thing to define. If you look at the CCPA, it has what I would consider to be a self-contradictory definition of aggregate information where it says it is a group of information that has been de-identified about individuals but it can't be a group of information about individuals that's been de-identified.

It's very hard to cabin but I would say ultimately that's what we want. We want to minimize privacy risks not just in terms of the use of information but if it's at rest. If you have it within your company, let's encourage anonymization. Let's encourage, you know, these new techniques that will help mitigate harm.

So I would want to make that a carve-out to any definition of personal sensitive information in the bill.

Senator MORAN. OK. Thank you.

Mr. BROOKMAN. I would largely agree. I mean, I think incentivizing companies to keep data at less-identifiable levels is good. De-identification is not perfect and like there will always be a small risk.

I generally support—the FTC announced a test for de-identification in 2012 or so. I think it's pretty thoughtful. Again, it's not perfect but I think it does—I'm willing to give companies reasons to keep de-identified data. I think that you can get value from data, yes, by keeping it less at less identifiable levels.

Senator MORAN. Mr. Brookman, I'm also an appropriator who appropriates money for the FTC. Would you like to fill in further about the need for additional resources?

Mr. BROOKMAN. Yes. So there are about 50 or so attorneys in the Division of Privacy and Identity Protection. Again, I think that they need—I mean, again, when there's a litigation going on or two litigations, then there are a considerable majority of attorneys are tied up in those and then everything else is relatively unregulated. So it's certainly attorneys in order to bring cases.

I was in the Office of Technology Research and Investigation, like the research wing in the technology wing, and we only had a handful of technologists, I think, at least in consumer protection. There may be, may be five full-time technologists. I think, you know, given the complexity of a lot of these practices, giving them considerably more people who understand how ad tracking works, how de-identification works, how AI works, I think is essential, so building out whether it's Bureau of Technology, open house structure, making sure they have both attorneys and technologists in order to, kind of, even barely keep up with these practices.

Senator MORAN. Thank you.

Senator Blumenthal.

Senator BLUMENTHAL. I have a question for you, Mr. Brookman.

Because you've raised the potential statute in Washington State, I think there has been a reference to North Dakota, what's on the horizon? What other states are moving forward in a serious way as opposed to, you know, a legislator throwing in a bill?

Mr. BROOKMAN. Certainly Washington State seems to be the most serious, though we and other consumer organizations have a lot of concerns with that bill.

I know Maryland had a hearing around this recently. I think we've seen—again, we don't have the resources to go to all these states. So I don't know how serious they are, but, I mean, I know a lot of folks are looking at CCPA and they're—like Mr. Engstrom said, it seems pretty reasonable, like we should have these, as well.

So I think probably, I mean, like Vermont had a bill on data brokers that turned into a study bill with the thought the bill tried to expand into a more serious bill later. So I think you're certainly going to see more and more states take action and I'm sympathetic to the idea about regulating the Internet especially in wildly different ways, but I think states are legitimately interested in offering protections for consumers over these issues that we all agree are problematic.

Senator BLUMENTHAL. Anyone have any other thoughts?

[No response.]

Senator BLUMENTHAL. Thank you.

Senator MORAN. Anything going on in Kansas or Missouri, Mr. Weber?

Mr. WEBER. You'd have to talk to lawmakers in both states. There's certainly tracking on this. They ask point blank do we need this in Kansas and Missouri and, of course, our response was wait and see how this progresses because again putting all this effort and work into a state law with Federal preemption looming is all for naught.

So there were no bills in both sessions that included privacy like this.

Senator BLUMENTHAL. Are you saying that Kansas is usually behind the rest of the country?

Mr. WEBER. No, sir. No, sir, I would not say that.

[Laughter.]

Senator BLUMENTHAL. I know it is not.

Senator MORAN. That's a poor recovery. Actually, my question, Senator Blumenthal, was going to ask the witnesses if they thought you and I and our team, Senator Wicker and Senator Schatz, were capable of coming up with a solution to this problem and therefore the likelihood of states waiting to see that——

Senator BLUMENTHAL. Well, Mr. Brookman has said that we operate very slowly.

Mr. BROOKMAN. I was talking about the institution more generally but I actually have been in to brief the working group and I've been totally impressed by how like dedicated and like deep in the weeds and how much good faith there is in trying to find a real solution. So I appreciate that.

Senator MORAN. A good answer came from my silly question. It was good. Thank you, Mr. Brookman.

Senator BLUMENTHAL. Well, we are very serious, I can assure you, and we have very able staff working on it and I think we have a good team.

Thank you.

Senator MORAN. Senator Blumenthal, thank you again for your cooperation in our working together.

We appreciate our witnesses joining us today to provide something that is very important. Innovation and startups is something that I've tried to champion since I came to the U.S. Senate and we wouldn't want to do something here that is damaging to that cause and your testimony has been helpful and balanced and all of you are articulate and intelligent. Thank you.

The hearing record will remain open for two weeks. During this time, Senators are asked to submit any questions that they have for the record. Those will then be submitted to the witnesses and upon receipt, the witnesses are requested to submit their written answers to the Committee as soon as possible.

This concludes our hearing, and we thank again our witnesses.

The hearing is adjourned.

[Whereupon, at 3:56 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO EVAN ENGSTROM

Question 1. Much of the discussion around privacy today concerns companies like Facebook sharing data with third parties such as Cambridge Analytica. But many small businesses share data with third parties that provide essential business services, like credit card processing.

Should a Federal consumer privacy law define such "service providers" distinctly from other "third parties" accessing personal information of consumers from a covered entity? Does anyone have any recommendations for Congress to appropriately account for these unique types of business arrangements?

Answer. Yes, a Federal consumer privacy law should differentiate between "third parties" and "service providers" that companies rely on to carry out everyday business functions. This differentiation is especially important to startups, which typically rely on widespread networks of service providers to deliver their products to users. Unlike large companies, startups don't have the resources to build these capacities in house, and limiting their ability to rely on and transfer data to service providers will severely impact their ability to compete with the world's largest tech companies.

The California Consumer Privacy Act attempts to solve this problem by carving out "service providers" serving "business purposes" from the definition of "sale." Unfortunately, the definition of "sale" is too broad, and the carve-outs are too narrow to protect all of the ways small companies rely on service providers. For instance, if a startup shares data with a website hosting platform about how users navigate the startup's website, and the platform then uses that data to make improvements across all of its offerings, that could be considered a sale under CCPA.

If a Federal bill were to include heightened consent requirements and protections around the actual sale of user data, many of the complications arising from this provision would be avoided.

Question 2. How should "de-identified" and "aggregated" consumer data be treated in the definition of "personal information" in a Federal consumer privacy bill?

Answer. Aggregated, anonymized, and de-identified data should be explicitly excluded from the definition of personal information in a Federal consumer privacy bill. In many circumstances, anonymized or aggregated data can provide the same value to startups for purposes of delivering, improving, and sometimes monetizing their services. When done correctly, using such data presents little in the way of privacy harms to consumers. A Federal bill should create—or direct the FTC to create—technological standards to ensure that the steps taken to aggregate, anonymize, and de-identify data can't be reversed to create new potential privacy harms.

Question 3. Your testimony described specific concerns with CCPA's broad definition of "sale" as it pertains to consumers' data. How will this overly inclusive definition harm each of your distinct memberships?

Answer. While we work with startups of all sizes across the country, Engine is an affiliated 501(c)(3)/(c)(4) research and advocacy organization that does not have a formal membership structure. Therefore, while we cannot speak to the practices or preferences of any specific companies, we have heard from many stakeholders that the CCPA's definition of "sale" covers many commonplace practices that businesses rely on to provide goods and services to consumers.

The law says that "releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information . . . to another business or a third party for . . . valuable consideration" constitutes a "sale" of data.

Several companies have told Engine that routine data sharing that presents no meaningful privacy harms could be included in the definition of sale due to the vague "valuable consideration" language. For example, we've heard from a local de-

livery platform that sharing order trends with local merchants to help those retailers stock their shelves in accordance with consumer demand could constitute a "sale" of consumer data under the law. In that case, the shared data would not contain personally identifiable information or otherwise be connected with any individual consumer, therefore posing no privacy risk.

The definition of sale does exclude some consumer data transfers to service providers, but the exemption provides limited protections because it relies on the narrow definitions of "service providers" and "business purposes," and prohibits service providers from retaining or using the data. For example, if a startup uses an e-mail delivery service to communicate with users and that service retains data provided by the startup to use in a manner that falls outside of the specific service the startup is requesting—such as making improvements to the software or building a list of defunct e-mail addresses—the law will see the startup as "selling" user data to the company running the e-mail delivery service.

The broad definition of sale will severely limit the ability of startups to rely on third party vendors to run their business processes. Unlike large companies, which typically have the resources to build these capacities in-house, startups rely on outside vendors for everything from data processing, to analytics, to payment processing.

Question 4. Your testimony described concerns around CCPA's requirements related to verification of consumer requests related to data. Specifically, you flagged that the state law "prohibits companies from requiring users to create an account in order to submit a verifiable request" to access or delete their information. Would you please further describe how this prohibition will lead to the unintended consequence of forcing companies to collect significantly more information to appropriately verify the source of the request?

Answer. If a company cannot use information it already has about a consumer—such as the information contained within the account the consumer has created with the company—it will need to find a different way to verify that the person making the request to access or delete information about a consumer is, in fact, the consumer whose data is at issue. There is simply no way for a company to determine the identity of a person requesting access to company-held data without collecting some personally identifiable information about that person. Companies that have no reason to collect such personally identifiable information to provide services would have to start collecting potentially sensitive personal information any time someone requested access to company-held information. This will almost certainly expand the range of personally identifiable information that companies must collect to stay compliant with CCPA. As one company we've talked to explained, "our worst nightmare is users e-mailing in pictures of their driver's licenses" to prove who they are.

This prohibition might make sense when dealing with entities like data brokers and other third-party companies that consumers never interact with and shouldn't have to provide additional information to in order to access and correct existing information about them held by the company, but applying it across the board to all companies will create unintended consequences. While the California Attorney General's rulemaking process will provide clarity on how companies can verify user identities without requiring requesters to create user accounts, it is inevitable that these rules will require companies to collect personally identifiable information that they may not currently collect.

Question 5. If Federal consumer privacy legislation includes a "small business exemption" like the CCPA, how should the Federal bill accommodate the "on ramp" mentioned in your testimony? More specifically, how should Congress set a deadline to become compliant with a Federal bill's privacy requirements should a small business surpass the "small business" thresholds overnight?

Answer. We would recommend giving companies a six-month grace period after meeting thresholds established in a Federal privacy law that remove them from a small business exemption. That will protect startups that suddenly become popular from finding themselves in violation of the law unexpectedly and without the resources to immediately mitigate the violation. More broadly, a small business exemption should recognize that the diversity of tech-enabled startup products and business models makes it impossible for any single factor to accurately determine a company's ability to shoulder the burdens and obligations of a privacy law. We recommend using a multi-factor test that takes into consideration the number of employees a company has, as well its revenue and number of users.

In a perfect world, a privacy law would be clear, straightforward, and consistent enough that companies of all sizes can afford to comply—especially recognizing that even a small company can create privacy harms depending on the sensitivity and scope of the consumer data it handles. However, any privacy law will create new

burdens and obligations on companies, and a tailored small business exemption can be written to ensure those burdens and obligations fall on small companies only when it makes sense, such as when a company collects particularly sensitive personal information.

Question 6. In terms of a Federal consumer privacy bill, I believe that consumers would benefit from Congress providing clear and measurable requirements in statutory text while also including appropriate flexibility in the form of narrow and specific rulemaking authority to the FTC to account for evolving technological developments. How should this committee approach providing the FTC with rulemaking authority?

a. Do you see value in making sure that there are strong "guardrails" around any rulemaking authority to preserve the certainty to the consumers that we aim to protect?

Answer. Engine supports Congress giving the FTC tailored rulemaking authority to protect consumer privacy online, and we see value in providing strong "guardrails" around rulemaking authority to preserve certainty that is crucial not only to consumers, but to startups and their investors as they attempt to launch and grow a business.

We support giving the FTC rulemaking authority to implement specific provisions of a Federal privacy law, including defining robust transparency requirements and outlining technological means to ensure anonymized, de-identified, and aggregated data stays that way to avoid privacy harms. We recognize that the FTC will need some flexibility to update requirements and prohibitions as technology evolves, but any additional requirements and prohibitions—including adding to the definitions of personal information, sensitive information, or discriminatory uses of data—should reflect actual harms faced by consumers and should be consistent with the goal of protecting consumers without putting startups at a competitive disadvantage to large incumbents.

Question 7. I have heard from many interested parties that the FTC currently lacks the resources needed to effectively enforce consumer privacy under its current Section 5 authorities. As a member of the Senate Appropriations Subcommittee with jurisdiction over the FTC, I am particularly interested in understanding the resource needs of the agency based on its current authorities, particularly before providing additional authorities. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

Answer. While we think the FTC is the correct body to write rules to implement a Federal privacy law and to enforce that law, we don't have specific recommendations for Congress to ensure that the FTC has the appropriations it needs to protect consumer privacy online, particularly since the resources necessary to adequately enforce a Federal law will vary depending on the substance of the law. We would support action by Congress to give the FTC the authority and resources it needs, but we defer to those with a better understanding of the agency's current resources when it comes to recommendations for additional appropriations.

Question 8. The Government Accountability Office (GAO) recently published a report in January regarding additional Federal authorities that could enhance consumer protections based on their review of past FTC privacy enforcement actions and input from industry, advocacy groups, and academia. One of the suggestions from GAO to enhance Internet privacy oversight was authorizing the FTC to levy civil penalties for first-time violations of the FTC Act. Would your organization and member companies support a Federal privacy bill that provides the FTC civil penalty authority? Why?

Answer. Engine would support a Federal privacy bill giving the FTC civil penalty authority if the bill creates clear, predictable, and consistent rules of the road around consumer privacy, and the penalties being issued by the FTC are related to the context of the violation, including the size of the company and the severity and impact of the violation.

Question 9. At its core, the 2012 FTC Privacy Framework is based upon providing consumers with notice regarding a company's privacy practices, giving consumers choice about how their personal information is collected, used and shared, and seeking consumers' consent based upon the sensitivity of their personal information. Does that type of model still make sense today?

Answer. The model laid out in the 2012 FTC Privacy Framework does make sense today, but as technology evolves and the collection, use, and sharing of consumer data becomes more complex, Congress has an opportunity to provide heightened protections that build off of that model. Those heightened protections include robust transparency requirements so that consumers really are informed about how their

data is being collected, used, stored, and shared, as well as outright prohibitions on particularly harmful uses of data, such as discriminatory profiling. Congress also has the opportunity to outline basic rights to correct, access, and delete information that consumers should have when it comes to the data they provide to companies.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELLEY MOORE CAPITO TO EVAN ENGSTROM

Question 1. Consumers have a right to know how their data is collected and used. How can we better educate individuals on data and their privacy rights and how their data is being used?

How will singular consumer control, as opposed to other methods, of their data cause economic problems for rural SME's? Can seniors be better educated? They are facing greater challenges.

Answer. Engine supports robust transparency requirements. Consumers should be able to learn what data is being collected and how it's used, stored, and shared. Companies should have clear and consistent guidelines—established by Congress or the Federal Trade Commission—as to how to explain their data collection, use, storage, and sharing practices in ways consumers, especially seniors, can understand.

Startups and small businesses across the country rely on consumer data to deliver and improve their products. Unlike large incumbents, startups and small businesses don't have existing vast datasets or the name recognition to build those datasets if their access to consumer data is cut off. While it's crucial that a Federal privacy framework give consumers more control over their data, there are many contexts in which companies understandably need—and users want to share—consumer data. Creating obstacles to that kind of data sharing will severely disadvantage small businesses, as compared to the large incumbents that already have consumer data or have enough market power to get data from consumers.

Question 2. Right now there is the potential for patch work state by state privacy regulations. Can you please describe what compliance would be like for your member-companies if there were 40 or 50 state consumer privacy laws?

Answer. While we work with startups of all sizes across the country, Engine is an affiliated 501(c)(3)/(c)(4) research and advocacy organization that does not have a formal membership structure. Therefore, while we cannot speak to the practices or preferences of any specific companies, we have heard from several small- and medium-sized companies that a patchwork of varying and potentially conflicting privacy laws at the state and local levels will be insurmountable, and will force companies to either stop offering their services in certain locations or sell their businesses to large incumbent technology companies that have the legal, budgetary, and technological resources to comply. Even if state laws are relatively consistent in terms of obligations for companies, the cost of updating vendor contracts to cover each new law would present massive costs for small companies. For many companies, contractual renegotiation was one of the more burdensome aspects of GDPR compliance, and multiplying that cost across dozens of jurisdictions would likely be too costly for many startups. Both of these outcomes will result in less competition and fewer innovative offerings for consumers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO NINA DOSANJH

Question 1. Should a Federal consumer privacy law define "service providers" distinctly from other "third parties" accessing personal information of consumers of a covered entity?

Answer. NAR believes that the level of protection for data should not depend on arbitrary distinctions between industries, such as whether a business directly collected data from a consumer or obtained it in a business-to-business transaction. Distinctions like "service provider" and "third party" are similarly arbitrary. Any entity who handles sensitive consumer data should be subject to the same uniform standards. Those standards should be direct statutory obligations for all entities handling consumer data. Federal privacy legislation should not include terms that could potentially expose businesses to liability for the actions or non-compliance of a business partner.

Question 2. How should "de-identified" and "aggregated" consumer data be treated in the definition of "personal information" in a Federal consumer privacy bill?

Answer. NAR does not have a position at this time on "de-identified" or "aggregated" data.

Question 3. How does the definition of "sale" in the CCPA harm REALTORS®?

Answer. The CCPA defines a "sale" of personal information in a manner that captures any arrangement in which a business not only sells but "rent[s]" or "make[s] available" personal information "for monetary or other valuable consideration" The breadth of this definition captures many types of data-sharing arrangements that are necessary in today's business environment and are not viewed by consumers as a "sale" of data. For example, REALTORS® may share data with vendors (photographers, postcard production, CRM) to help market a client's home or to help determine a competitive sales price. This could be considered a "sale" under CCPA and limitation of this activity would significantly harm our members' ability to serve their clients in a manner they have come to expect.

Question 4. How should this committee approach providing the FTC with rulemaking authority? Do you see value in making sure there are strong "guardrails" around any rulemaking authority to preserve the certainty to consumers that we aim to protect?

Answer. The Federal Trade Commission (FTC) should have the appropriate authority to enforce comprehensive privacy regulations. NAR appreciates that the FTC employs a scalable reasonableness approach that determines the appropriateness of business practices in light of the size of the business and the sensitive nature of the data they process under Section 5 of the FTC Act. Any future privacy legislation should ensure that the FTC continues to employ flexibility in their implementation of reasonable privacy standards that will permit the Commission to enforce such regulations fairly and equitably to ensure businesses' compliance with them and to promote robust consumer protection.

Question 5. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

Answer. The FTC should be given the resources necessary to fund their enforcement mission. NAR believes the FTC is best able to determine those funding requirements.

Question 6. Would your organization and its members support a Federal privacy bill that provides the FTC civil penalty authority? Why?

Answer. NAR has concerns with FTC civil penalty authority and the potential for creating "privacy trolls." Unless litigation reforms are included that would require plaintiffs to provide sufficient information at the initiation of a lawsuit, provide early discovery and other reforms, creation of civil penalty authority could create an environment similar to "patent trolling" where unscrupulous actors game the system to bring frivolous lawsuits that could easily put small business owners out of business.

Question 7. Does the notice and choice model still make sense today?

Answer. Notice and choice does make sense and can be improved. Consumers deserve to know what categories of personal data that businesses collect and how that data is generally used by them. These policies should be clearly disclosed in company privacy policies and readily accessible to consumes looking to learn how their data is collected and used. Federal data privacy law should provide the regulatory flexibility necessary to ensure that transparency in privacy policies is provided to consumers without unnecessarily burdening businesses with requirements to seek consumer consent when they are continuing to use data based on reasonable consumer expectations.

Question 8. What are some key items we should include or avoid in order to craft legislation that is both effective and efficient? Why will CCPA and GDPR create highly burdensome compliance costs for rural businesses?

Answer. NAR's top priority for any new Federal privacy law is ensuring that Congress craft realistic compliance requirements for small businesses and independent contractors. Regulations should consider the size of the business, the nature and sensitivity of the information collected and how the information is used. Regulations should be narrowly tailored to target behavior that goes beyond reasonable consumer expectations or that can cause demonstrable harm to consumers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO JUSTIN BROOKMAN

Question 1. Much of the discussion around privacy today concerns companies like Facebook sharing data with third parties such as Cambridge Analytica. But many small businesses share data with third parties that provide essential business services, like credit card processing.

Should a Federal consumer privacy law define such "service providers" distinctly from other "third parties" accessing personal information of consumers from a covered entity? Does anyone have any recommendations for Congress to appropriately account for these unique types of business arrangements?

Answer. Consumer Reports supports privacy legislation that reasonably accommodates the use of external service providers by largely excluding such transfers from the definition of third-party sharing. If data is shared for a limited operational business purpose, and the service provider is prohibited from secondary usage of the data for its own benefit, it makes sense to think of such processing as first-party collection, use, and retention.

Of course, sharing data with service providers necessarily exposes consumers to additional risk of breach or misuse. And logical siloing of data from different data partners may not provide much in the way of practical protections. For this reason, companies should be transparent about their use of service providers, and should disclose detailed information about how they are used within privacy policies (including, where practicable, specifically identifying what providers get what information). Moreover, service providers should be subject to the same reasonable data security requirements that should govern companies with a direct consumer relationship. Finally, service provider use of customer data should be limited to the parameters of the first-party interaction. For example, if a privacy law prohibits data sharing (whether by default or as a result of a consumer exercising a choice), a company should not be able to provide ad targeting data to a service provider in order to display retargeting ads on different websites.

Question 2. How should "de-identified" and "aggregated" consumer data be treated in the definition of "personal information" in a Federal consumer privacy bill?

Answer. While they are imperfect protections, deidentification and aggregation are useful tools to protect personal data from exposure and misuse, and privacy law should certainly encourage companies to keep data in less identifiable forms. In general, the FTC's three-part test enunciated in its 2012 privacy report is sound: (1) companies must use technical measures such that they reasonably believe that the data could not be tied back to an individual or device, (2) the company must publicly commit to not try to reidentify the data, and (3) anyone with whom the data is shared must also commit to not try to reidentify the data.[1]

Of course, many ostensible anonymization techniques are not robust enough to sufficiently obscure data, and they should not be regarded as render data deidentified: for example, simply hashing identifiers will not meaningfully deidentify data in most cases.[2] Companies should be incentivized (or compelled) to be transparent about the methods deidentify data in order to provide for external accountability. Moreover, while companies should be permitted to use deidentified data more expansively than personal data, not all obligations should go away. For example, companies should still have to use reasonable security to prevent access to persons who have not committed to not reidentify the data. There also may be some uses of deidentified data that may be inconsistent with reasonable consumer preferences and expectations, especially if the data is being used to alter the individual's experience outside the context of his relationship with the company who originally collected the data (say, for example, to serve targeted ads based on that data in a different environment).[3]

Question 3. In terms of a Federal consumer privacy bill, I believe that consumers would benefit from Congress providing clear and measureable requirements in statutory text while also including appropriate flexibility in the form of narrow and specific rulemaking authority to the FTC to account for evolving technological developments. How should this committee approach providing the FTC with rulemaking authority?

a. Do you see value in making sure that there are strong "guardrails" around any rulemaking authority to preserve the certainty to the consumers that we aim to protect?

Answer. We agree that legislation should give the FTC rulemaking authority to provide more clarity to businesses and consumers as technologies and business practices evolve. Given the limitations of resources, a clear statement of industry-wide

---

[1] Report, Protecting Consumer Privacy in an Era of Rapid Change, Fed. Trade Comm'n, (March 2012), *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-cons umer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.*

[2] Ed Felten, *Does Hashing Make Data "Anonymous"?,* Fed. Trade Comm'n, (Apr. 22, 2012), *https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous.*

[3] *E.g., About Custom Audiences from customer lists,* Facebook, *https://www.facebook.com/business/help/341425252616329.*

obligations and responsibilities in a regulation may be more effective than in establishing norms through the settlement of cases or caselaw through the courts. One reasonable guardrail around FTC rulemaking would be to make it discretionary rather than mandatory, so that the FTC would only issue regulations when it has identified a clear need. Moreover, Congress can obviate the need for rulemaking by writing clear and simple rules that do not require clarification from the Commission, or at least specifying the factors should inform rulemaking.

The best approach would be to give the FTC the discretion to issue rules as they see fit to give them the most flexibility to respond to marketplace needs. However, Congress could also specify particular areas as examples where rulemaking may be most appropriate. One area where the FTC could issue helpful guidance is around user interfaces and consent, in order to create standardized language that becomes familiar to consumers, and to more effectively prohibit the use of "dark patterns" to unfairly manipulate decisions and frustrate user agency. Reasonable data security may be another area where the FTC can issue specific guidance over time to give companies more certainty than the relatively high-level requirements that are more appropriate to a statute.

Question 4. I have heard from many interested parties that the FTC currently lacks the resources needed to effectively enforce consumer privacy under its current Section 5 authorities. As a member of the Senate Appropriations Subcommittee with jurisdiction over the FTC, I am particularly interested in understanding the resource needs of the agency based on its current authorities, particularly before providing additional authorities. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

Answer. The FTC certainly needs a massive influx of resources in order to achieve its broad consumer protection mission; its chronic understaffing problem is *not* limited to privacy. However, on privacy specifically, the current staff of 40 FTEs dedicated to privacy is woefully insufficient, and pales in comparison to other data protection authorities around the world (who serve far smaller economies and populations).[4] A good start would be to expand the Division of Privacy and Identity Protection to 200 FTEs while also expanding the current Office of Technology Research and Investigation into a full-fledged Bureau of Technology with 100 FTEs to serve all of the Commission's staff in their work. But regardless of structure, hiring a substantial and diverse array of cross-functional staff to augment the Commission's privacy resources is absolutely essential.

However, it is important to point out that resources alone will not empower the FTC to sufficiently police companies' privacy behaviors. The FTC today generally pursues privacy cases under its general Section 5 prohibition on deceptive and unfair business practices. In response, companies have generally evaded responsibility for bad privacy practices by simply saying as little as possible about what they are doing, thus avoiding saying anything the FTC could prove is untrue. While the FTC could be more aggressive in arguing "deceptive omissions"—or more promisingly—"unfairness," its legal authority here is not clear for either consumers or businesses. In order to deliver to consumers the privacy rights they want and expect, Congress must pair enforcement resources with new, clear substantive protections.

Question 5. The Government Accountability Office (GAO) recently published a report in January regarding additional Federal authorities that could enhance consumer protections based on their review of past FTC privacy enforcement actions and input from industry, advocacy groups, and academia. One of the suggestions from GAO to enhance Internet privacy oversight was authorizing the FTC to levy civil penalties for first-time violations of the FTC Act. Would your organization support a Federal privacy bill that provides the FTC civil penalty authority? Why?

Answer. The FTC should absolutely be empowered to seek penalties from any company that violates Section 5 or a new privacy statute: companies shouldn't be entitled to one automatic "get out of jail free" card, only facing significant consequences for wrongdoing when they had previously been subject to an enforcement action. Nearly all civil and criminal statutes today carry consequences for "first-time" violations; the FTC is an extreme outlier in this regard (certainly compared to state Attorneys General who can obtain "first-time" penalties under their versions of Section 5). That said, penalties are discretionary, and the Commission or the courts may reasonably take into account the fact that a defendant had not pre-

[4] Letter from Chairman Joe Simons to Chairman Pallone, (Apr. 1, 2019), *https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/FTC%20Response%20to%20Pallone-Schakowsky.pdf.*

viously been charged with similar wrongdoing in the past in assessing appropriate remedies.

Similarly, Consumer Reports has strongly objected to language giving companies a "right to cure" privacy violations before liability attaches. This a regrettable element of the recently enacted California Privacy Protection Act, though we have supported legislation to eliminate that provision.[5] Many bad privacy practices are completely invisible and undetectable by consumers: under this provision, a company could egregiously violate the law, and only cease its behavior once its privacy-invasive practices were found out—with no more consequence than to have to stop breaking the law. Companies should not have to receive notice from the Federal Trade Commission before being legally responsible for following the law.

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

Answer. No, the model did not make sense then, and it does not make sense now. Privacy policies—especially absent affirmative transparency obligations—are not an effective means of informing consumers, and consumers are certainly not consciously agreeing to opaque and inscrutable data practices merely by going online or going about their daily lives. What is sometimes described as "notice-and-choice" is in fact neither.

A better model would be premised on reasonable *data minimization* or *focused collection and sharing*. That is, companies should collect and share the data that is reasonably necessary for a particular transaction or relationship—without clunky consent screens and invasive interfaces—but not more. The company would be permitted some narrow first-party secondary uses of that data—such as for analytics, measurement, fraud prevention, and marketing—but consumers wouldn't have to worry that everything they do on-or off-line was being shared indiscriminately with dozens of data brokers and ad tech companies. So if I purchase something online, the company collects the data that is reasonably needed to effect the purchase, uses that data internally for specified business purposes, and can share my data with a shipping company—all without special consent. But they shouldn't be allowed to sell information about my shopping behavior to data brokers or third-party marketers. Similarly, Facebook can collect and use data about what I do on Facebook, but they shouldn't be monitoring what users do on other websites, in other mobile apps, and in the physical world (unless necessary for a feature the consumer has chosen to enable).

On the other hand, frameworks that rely primarily upon *corporate accountability* or *risk management* would be a step backwards for privacy protection and would favor big businesses over smaller competitors. These models rely extensively on opaque and conflicted decision-making within companies about what privacy protections and rights to offer consumers, and prioritize privacy process over substantive rules. As such, they provide few reliable protections for consumers, and advantage existing companies with the resources to pay lawyers to document and justify complex data practices. Instead, privacy rules should be simple and straightforward, offering clarity and consistency for both consumers and companies.

○

[5] Letter from Justin Brookman and Maureen Mahoney to Chair Jackson re SB 561, California Consumer Privacy Act of 2018, Consumer Remedies (Jackson)—SUPPORT, (Apr. 3, 2019), *https://advocacy.consumerreports.org/wp-content/uploads/2019/04/Consumer-Reports-SB–561-Support.p df.*