Opening Statement of Republican Leader Cathy McMorris Rodgers
Subcommittee on Consumer Protection and Commerce
"Protecting Consumer Privacy in the Era of Big Data"
February 26, 2019

As Prepared for Delivery

Good morning and welcome to our first Consumer Protection and Commerce Subcommittee hearing. I would like to congratulate Chair Schakowsky. I would also like to recognize the newest Members of the Subcommittee, Mr. Hudson from North Carolina, Mr. Carter from Georgia, and Mr. Gianforte from Montana. I look forward to working with all of the Members this Congress. Our jurisdiction includes vast portions of the economy and I look forward to working with you on bipartisan solutions that improve the lives of all Americans.

I also would like to thank the Chair for organizing this first hearing of the Congress on privacy and security. This hearing builds on the good work of Chairmen Walden and Latta in the last Congress, and Chairmen Upton and Burgess in the 114th Congress. While there have been issues achieving bipartisan consensus in the past, I'm encouraged that we can find a bipartisan path forward on a single American approach to privacy - one that supports free markets, consumer choice, innovation and small businesses---the backbone of our economy.

Principle #1: One National Standard

The Constitution was crafted around the concept that one national marketplace would make America stronger in certain areas. It also recognizes the

importance of intellectual property rights, free expression, and the rights of "We, the People" to be protected from the power of the government. The Internet knows no borders. It has revolutionized our nation's economy by seamlessly connecting businesses and people across the country.

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

Principle #2: Transparency and Accountability

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

Principle #3: Improving Data Security

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

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

Principle #4: Small Businesses

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

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

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

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

As we continue to explore data privacy and security, we must find a forward-thinking solution that fosters innovation and protects consumers from bad

data practices that have caused people harm or create real risks. By achieving both, America will maintain our robust internet economy and continue to be the best place in the world to innovate.

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