Opening Statement of Ranking Member Jan Schakowsky
House Energy and Commerce Committee
Subcommittee on Digital Commerce & Consumer Protection
Hearing on "21st Century Trade Barriers: Protectionist Cross-Border Flow Policies' Impact on U.S. Jobs"

October 12, 2017

Thank you, Chairman Latta. The Internet has made our world dramatically more connected than ever before. It facilitates the exchange of ideas, keeps families and friends connected, and creates new opportunities for global commerce.

Over 2.3 billion people have access to the Internet, and this figure is expected to grow to 5 billion by 2020. Digital commerce comprises a growing share of the global economy. In fact, a McKinsey report claims that "[s]oaring cross-border data flows now generate more economic value than traditional flows of traded goods."

Cross-border data flows allow for quick communication – whether it is a personal message or a customer order. It also introduces additional risks to consumer privacy and data security.

Global digital commerce has become a necessity in the U.S. economy. Although the Internet is global, the rules governing data are not. Differences among countries can create challenges for businesses and consumers. Countries should not be dissuaded from protecting their citizens' privacy and security. But some of the policies we see across the world today are counterproductive to data security and privacy. Requiring local servers can create new security risks. The U.S. should also not empower regimes that monitor or restrict flow of data as a limit on their citizens' rights to free speech and expression.

We need to distinguish between policies that truly present an unnecessary or harmful barrier to digital trade and those policies designed to protect privacy and security.

When it comes to data privacy and security, current U.S. law is lacking.

We heard a clear example of that last week when former Equifax CEO Richard Smith testified in front of our committee. By failing to patch a known vulnerability, Equifax allowed the data of 145.5 million Americans to be compromised. I still have a lot of questions about that breach. Today, my Democratic colleagues and I are sending a letter requesting additional hearings to get the answers that Americans deserve.

The Equifax breach impacted not only Americans but also consumers outside of the United States. So you can understand if consumers – and governments – abroad have their doubts about the data practices of American companies. That is yet another reason why we need action in Congress to improve data security.

Last week, I introduced the Secure and Protect Americans' Data Act to ensure that companies take sufficient steps to protect consumers' data, promptly notify law enforcement and consumers if a data breach occurs, and provide meaningful relief to breach victims.

Digital trade partners are also concerned about U.S. surveillance practices. Section 702 expires at the end of this year, and we should take this opportunity to better protect privacy while still providing for our nation's security.

As we strengthen our own laws, we need to continue engaging with partners such as the European Union on ways to facilitate cross-border data flows while ensuring that consumers here and abroad enjoy the privacy and security they expect.

The U.S. benefits greatly from digital trade, and we should work to keep data flowing across borders. That requires improving our own laws and engaging with other nations on how to keep consumers' data and rights protected. I look forward to hearing from our witnesses and getting your perspectives on this complex issue.