

**Statement of Ranking Member Frank Pallone, Jr.  
House Committee on Energy and Commerce  
Subcommittee on Digital Commerce and Consumer Protection  
Hearing on “21st Century Trade Barriers: Protectionist Cross  
Border Data Flow Policies Impact on U.S. Jobs”**

*September 12, 2017*

Today’s hearing is about the policies of foreign governments that affect the free flow of information across national boundaries.

There is no dispute that the United States leads the world in technological innovation. And data continually crossing national borders is critical to that status.

Most of us don’t spend much time thinking about how data is stored, how it moves, or how it affects our daily lives. But in our digital society, we rely on the ability of data to move quickly and seamlessly. It is essential to American innovation and enterprise.

Businesses of all types and sizes, and in virtually all industries, rely on data flows. For example, this near-instantaneous data flow happens when you use a credit card in another country to buy a sandwich or when you purchase a product from a company located overseas online. All sectors, including agriculture, mining, and manufacturing, are reliant on moving data.

The free flow of data allows business to flourish both domestically and abroad. Unnecessary barriers to these data flows affect the American economy and American jobs.

In recent years, a number of countries have begun to put policies in place that may hamper the free flow of information. Data localization policies take a number of forms, from explicit requirements that data be stored and processed within a country's borders to prohibitions on the transfer of personal information to countries that do not have adequate levels of data protection.

Governments assert a number of reasons for data localization policies. Concerns about law enforcement access to individuals' personal information have gotten a lot of attention in recent years following the disclosure of the NSA's surveillance programs.

Other factors are also at play—factors like competitiveness and antitrust concerns. In addition, national security and law enforcement interests have only increased in the wake of recent terror attacks all over the world. And some policies may be purely protectionist—to attempt to give local companies competitive advantage.

Like most Americans, citizens of other countries are troubled by the mass collection of personal information by private companies and whether that information is kept secure. Massive data breaches—like the Equifax breach, which affects British and Canadian citizens in addition to Americans—makes people even more nervous about their personal privacy. Enacting baseline consumer privacy and data security protections in this country can help ease those fears.

Meanwhile, addressing the other concerns of foreign citizens and foreign governments—those based on national security or economics—may require a combination of government and commercial actions to prevent harmful restrictions on cross border data flows.

I look forward to hearing from our witnesses on this important topic. Thank you.