FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

September 16, 2014

To: Subcommittee on Commerce, Manufacturing, and Trade Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?"

On Wednesday, September 17, 2014, at 1:30 p.m. in room 2322 of the Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing titled "Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?"

I. BACKGROUND

Cross-border data flows refer to the electronic movement of information across national boundaries.[1] At any moment, immense amounts of electronic data flow in real time through networks of computers, servers, and data storage systems that process and store the data, including some that are cloud-based.[2] Each component of these networks may be located in different countries and different continents; data can cross borders without the knowledge of the

[1] William L. Fishman, *Introduction to Transborder Data Flows*, 16 Stan. J. Int'l L. 1 (1980).

[2] Electronic Privacy Information Center, *Cloud Computing* (online at epic.org/privacy/cloudcomputing) (accessed Sept. 14, 2014). Cloud computing, which the majority of American adults use daily without much notice on their smartphones, means simply "storing and accessing data and programs over the Internet instead of your computer's hard drive." Pew Research Internet Project, *Mobile Technology Fact Sheet*, (online at www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet) (accessed Sept. 15, 2014); Eric Griffith, *What is Cloud Computing?*, PC Magazine (Mar. 13, 2013).

sender or the recipient.[3] In addition, e-commerce is routinely conducted on an international scale, which leads to consumers' personal information being transferred across borders.

Cross-border data flows are necessary to the modern U.S. economy, with benefits for both producers and consumers.[4] Nearly every industry is affected in varying degrees by data transfer over the Internet, including not only information and communications technologies and retail, but also a broader range of industries, such as manufacturing, financial services, utilities, and healthcare.[5] The Internet has allowed producers of goods and services to have a global reach, allowed mid-sized and small businesses to have access to global markets, and transformed some types of goods (such as books, television, and movies) into digital data.[6] The value of e-commerce is estimated at $8 trillion per year.[7] Digital trade-related exports totaled $356.1 billion in 2011, up from $282.1 billion in 2007.[8]

II. SAFETY, SECURITY, AND PRIVACY

The open flow of information raises safety, security, and privacy concerns. Cloud-based processing and storage removes control of security of content from end users.[9] Information that was once stored on the user's hard drive is now transferred through the Internet and stored on cloud computing service providers' servers, which increases the risk of access by unwanted parties.[10]

---

[3] Joshua Meltzer, *The Internet, Cross-Border Data Flows, and International Trade*, Issues in Technology Innovation (Feb. 2013).

[4] United States International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1* (July 2013) (Investigation No. 332-531).

[5] *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, U.S. Chamber of Commerce (Apr. 15, 2013) (online at www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf); United States International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1* (July 2013) (Investigation No. 332-531).

[6] Karen Kornbluh, *Beyond Borders: Fighting Data Protectionism*, Democracy: A Journal of Ideas (Fall 2014) (online at www.democracyjournal.org/34/beyond-borders-fighting-data-protectionism.php?page=all).

[7] *Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity*, U.S. Chamber of Commerce and Hunton & Williams (2014) (online at www.uschamber.com/sites/default/files/021384_BusinessWOBorders_final.pdf).

[8] United States International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1* (July 2013) (Investigation No. 332-531).

[9] Electronic Privacy Information Center, *Cloud Computing* (online at epic.org/privacy/cloudcomputing) (accessed Sept. 14, 2014).

[10] *Id.*

In the U.S., under current law, the requirement to secure and keep private other people's data, including digital data, is seen as sector-specific. For example, there are specific requirements on personal health data, financial institutions, and the collection of information about children.[11] However, there is no federal law in the U.S. providing comprehensive privacy or data security protections to consumers. In addition, while there is generally a prohibition against government access, there are a number of laws that allow such access to personal data in certain circumstances.[12]

Compared to the U.S., many countries take very different approaches to privacy and data security. In the European Union, for example, privacy and data security is governed in large part by the EU Data Protection Directive, which established a framework that member states must meet for the collection and processing of personal data in Europe and sets a baseline for the required security of the storage, transmission, and processing of personal information.[13] The EU is in the process of developing a unified General Data Protection Regulation, which would replace the Directive, establish a single set of rules for all EU member states, and expand data protection requirements on foreign companies. Laws on government access to personal data vary across countries. For example, in France, government access to personal communications is prohibited except in cases of national security, counter-terrorism, and, under a new law, to protect the scientific and economic potential of France.[14]

III. BARRIERS TO DIGITAL TRADE

In recent years, several countries have considered laws that restrict cross-border data flows.[15] In addition to data privacy and security measures that may place requirements on data transferred abroad, these proposals include the compelled domestic storage of citizen data (or

---

[11] Government Accountability Office, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace* (Sept. 25, 2013) (GAO-13-663).

[12] *See, e.g.*, the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508; the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511; the USA PATRIOT Act, Pub. L. No. 107-56 (2001); and Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981).

[13] Marc Rotenberg and David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, Harvard Journal of Law and Public Policy (Spring 2013).

[14] *New French Surveillance Law: From Fear to Controversy*, Computer World (Jan. 7, 2014).

[15] In fact, some countries have already passed laws requiring data generated within the country to be stored on servers located in the country. United States International Trade Commission, Testimony of Information Technology & Innovation Foundation, *Hearing on Digital Trade in the U.S. and Global Economies*, Investigation No. 332-531 (Mar. 14, 2014). Even in the United States, some state regulators require their licensees to keep all customer data within the state. New York City Bar Association Committee on Small Law Firms, *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations* (Nov. 2013).

forced data localization), intellectual property-related regulations, online censorship, and traditional trade barriers.[16] Sometimes these measures are motivated by what is seen as a need to regulate potential harms to citizens and consumers.[17] However, these proposals also can be motivated by unrelated issues such as an interest in promoting local business over foreign competition, by a government interest in inhibiting external political influence, or by a desire for continued domestic government surveillance.[18]

Revelations last year related to the apparent Internet surveillance programs of the National Security Agency (NSA) increased international support for greater local control of Internet traffic and network infrastructure.[19] Now, more than a dozen countries have introduced or are discussing forced data localization laws and other digital trade barriers specifically designed to inhibit transfer of information across borders.[20]

Recent industry reports suggest that actual data transfer restrictions, and even the threat of such restrictions, have both direct and indirect costs on American companies.[21] In addition to the implementation of new policies with significant compliance costs, recent surveillance revelations have caused foreign clients to lose trust in U.S.-based business, particularly in the information and communications technology sector.[22] This loss of trust has led to direct economic costs. U.S. companies report losing business to local companies that market products and services as "NSA-proof" or as "safer" alternatives to American-produced goods and services.[23]

IV. TRADE NEGOTIATIONS AND CROSS-BORDER DATA FLOWS

Recent developments regarding international data flows may have a particular impact on international agreements between the United States and foreign governments. Data transfer between the EU and U.S. is currently governed by a Safe Harbor Framework, which provides a method for U.S. companies to transfer personal data outside of Europe in a way that is consistent

---

[16] United States International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1* (July 2013) (Investigation No. 332-531).

[17] Joshua Meltzer, *The Internet, Cross-Border Data Flows, and International Trade*, Issues in Technology Innovation (Feb. 2013).

[18] *Id.*

[19] Danielle Kehl et al., *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, & Cybersecurity*, Open Technology Institute (July 2014).

[20] *Id.*

[21] *Id.*; *Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity*, U.S. Chamber of Commerce and Hunton & Williams (2014) (online at www.uschamber.com/sites/default/files/021384_BusinessWOBorders_final.pdf).

[22] Danielle Kehl et al., *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, & Cybersecurity*, Open Technology Institute (July 2014).

[23] *Id.*

with the EU Data Protection Directive.[24] To join, a company must comply with the Safe Harbor's requirements and annually self-certify to the Department of Commerce that it agrees to comply with the requirements.[25] The Department of Commerce and European Union are currently negotiating changes to the Safe Harbor program.[26]

Negotiations are now underway for three trade agreements intended to modernize trade rules in an increasingly digital global economy. Keeping open digital trade and cross-border data flows has been an important topic of comments and conversation regarding each of the major proposed trade agreements. The purpose of these proposed agreements is to reduce or eliminate tariffs and other trade barriers and to harmonize varying regulations, where possible.[27]

In the Pacific region, the U.S. has been involved in developing and negotiating the Trans-Pacific Partnership (TPP) with 11 other countries in the Asia-Pacific region for more than five years.[28] The U.S. and the EU are engaged in discussions over an agreement known as the Transatlantic Trade and Investment Partnership (TTIP) that is focused on reducing the few remaining tariffs and ensuring greater compatibility in regulations enforced by the two regions.[29] The Trade in Services Agreement (TISA) is an agreement currently being negotiated to promote fair and open trade in the service sectors of 50 participating countries or regions representing 65% of the global services market.[30]

V. WITNESSES

The following witnesses have been invited to testify:

---

[24] Federal Trade Commission, *U.S.-EU Safe Harbor Framework* (online at www.business.ftc.gov/us-eu-safe-harbor-framework) (accessed Sept. 14, 2014).

[25] Export.gov, *U.S.-EU Safe Harbor Overview* (online at www.export.gov/safeharbor/eu/eg_main_018476.asp) (accessed Sept. 14, 2014).

[26] *EU Cites U.S. Data Transfer Pact Progress Amid Privacy Regulation Reform Negotiations,* Bloomberg BNA (June 9, 2014) (online at www.bna.com/eu-cites-us-n17179891134).

[27] *Everything you need to know about the Trans Pacific Partnership*, Washington Post (Dec. 11, 2013) (online at www.washingtonpost.com/blogs/wonkblog/wp/2013/12/11/everything-you-need-to-know-about-the-trans-pacific-partnership).

[28] Office of the United States Trade Representative, *Trans Pacific Partnership* (online at www.ustr.gov/tpp) (accessed Sept. 11, 2014). The other countries that are part of the TPP are Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam.

[29] Office of the United States Trade Representative, *Transatlantic Trade and Investment Partnership (T-TIP)* (online at www.ustr.gov/ttip) (accessed Sept. 11, 2014).

[30] United States Trade Representative, *Remarks as Prepared for Delivery by Ambassador Michael Froman at the Coalition of Services Industries on the Trade in Services Agreement* (June 18, 2014).

Brian Bieron
Executive Director, Global Public Policy
eBay Incorporated

Linda Dempsey
Vice President, International Economic Affairs
National Association of Manufacturers

Laura Donohue
Professor of Law, Georgetown University Law Center
Director, Center on National Security and the Law

Sean Heather
Vice President, Center for Global Regulatory Cooperation
U.S. Chamber of Commerce