GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH 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

October 10, 2017

To: Subcommittee on Digital Commerce and Consumer Protection Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies Impact on U.S. Jobs"

On **Thursday, October 12, 2017, at 10:15 a.m. in room 2322 of the Rayburn House Office Building**, the Subcommittee on Digital Commerce and Consumer Protection will hold a hearing titled "21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies Impact on U.S. Jobs." The subcommittee has held two previous hearings on this topic.[1]

I. BACKGROUND

Cross-border data flows refer to the electronic movement of information across national boundaries.[2] Immense amounts of electronic data are continually flowing in real time through networks of computers, servers, and data storage systems that process and store the data.[3] Components of these networks may be located in different countries and data can cross borders without the knowledge of the sender or the recipient.[4]

[1] The memos for these prior hearings can be found here and here.

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

[3] Electronic Privacy Information Center, *Cloud Computing* (epic.org/privacy/cloud computing) (accessed Sept. 7, 2017).

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

Cross-border data flows are necessary to the modern U.S. economy, with benefits for both producers and consumers.[5] All sizes of companies in nearly every industry are affected by data transfer over the Internet, including manufacturing, financial services, utilities, and healthcare.[6]

II. PRIVACY AND DATA SECURITY

The open flow of information raises safety, security, and privacy concerns. 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.[7]

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. In addition, while there is generally a prohibition against government access, a number of laws allow such access to personal data in certain circumstances.[8]

Compared to the U.S., many countries take very different approaches to privacy and data security. The EU has developed a unified General Data Protection Regulation, which establishes a single set of rules for all EU member states and expands data protection requirements on foreign companies.[9] Laws on government access to personal data vary across countries. For example, in the wake of terrorist attacks in Europe, some European countries have passed laws allowing for increased large-scale government surveillance of communications.[10]

---

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

[6] *Id*.; *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, U.S. Chamber of Commerce (Apr. 15, 2013) (www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf); Karen Kornbluh, *Beyond Borders: Fighting Data Protectionism*, Democracy: A Journal of Ideas (Fall 2014).

[7] *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, U.S. Chamber of Commerce (Apr. 15, 2013) (www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf).

[8] *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).

[9] *GDPR Will Change Data Protection –Here's What You Need to Know*, Wired (Sept. 5, 2017) (www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018).

[10] *A New Era of Mass Surveillance is Emerging Across Europe*, Medium (Jan. 17, 2017) (medium.com/privacy-international/a-new-era-of-mass-surveillance-is-emerging-across-europe-3d56ea35c48d).

In July 2017, the European Commission adopted the EU-U.S. Privacy Shield framework. The framework allows companies to move commercial digital information between the U.S. and Europe by providing a mechanism by which companies can comply with European privacy regulations.[11] The agreement requires annual joint reviews of the functioning of the Privacy Shield conducted by the European Commission, the U.S. Department of Commerce, and the Federal Trade Commission.[12] The first of these reviews took place on September 18-19, 2017, and a report is expected in late October.[13] In a June 15, 2017, letter, the Article 29 Working Party, an independent advisory body made up of representatives of each member states' supervisory authorities, laid out a number of concerns it wants addressed by the review, and requested the participation of a number of additional federal agencies, including the Department of Transportation.[14] The Privacy Shield continues to face skepticism and scrutiny from some European officials, privacy advocates, and others.[15]

III. BARRIERS TO DIGITAL TRADE

In recent years, several countries have enacted laws compelling the domestic storage and processing of data that restrict cross-border data flows.[16] Sometimes these measures are motivated by 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 or by a desire for continued domestic government surveillance.[18] For example, Indonesia mandates that companies maintain servers within the country for access by law enforcement agencies in the name of national security.[19]

---

[11] *EU-US Privacy Shield Now Officially Adopted but Criticisms Linger*, Tech Crunch (Jul. 12, 2016) (techcrunch.com/2016/07/12/eu-us-privacy-shield-now-officially-adopted-but-criticisms-linger/); U.S. Department of Commerce, Fact Sheet Overview of the EU-U.S. Privacy Shield Framework (www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu-us_privacy_shield_fact_sheet.pdf) (accessed Sept. 7, 2017).

[12] Letter from Article 29 Data Protection Working Party to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission (June 15, 2017).

[13] European Parliament, *Answer given by Ms Jourová on behalf of the Commission* (Oct. 5, 2017) (www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2017-005193&language=EN).

[14] *See* note 12.

[15] *Privacy Shield Is Already Coming Apart at the Seams*, Irish Times (Sept. 7, 2017) (www.irishtimes.com/business/technology/privacy-shield-is-already-coming-apart-at-the-seams-1.3211790).

[16] *Rising Demands for Data Localization a Response to Weak Data Protection Mechanisms*, Electronic Frontier Foundation (Aug. 14, 2017) (www.eff.org/deeplinks/2017/08/rising-demands-data-localization-response-weak-data-protection-mechanisms).

[17] *See* note 3.

[18] *Id.*

[19] *See* note 16.

Recent industry reports suggest that actual data transfer restrictions, and even the threat of such restrictions, have financial effects on American companies.[20] The implementation of new policies significantly increases compliance costs.[21] These costs can be significant for small and medium-sized businesses.[22] In addition, mistrust of American companies' cooperation with law enforcement has led to economic losses.[23]

IV. WITNESSES

The following witnesses have been invited to testify:

Jennifer Daskal
Associate Professor
American University Washington College of Law

Victoria A. Espinel
President and Chief Executive Officer
BSA-The Software Alliance

Dean C. Garfield
President and Chief Executive Officer
Information Technology Industry Council

Morgan Reed
President
ACT-The App Association

[20] *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, & Cybersecurity*, Open Technology Institute (July 2014).; *Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity*, U.S. Chamber of Commerce and Hunton & Williams (2014) (www.uschamber.com/sites/default/files/021384_BusinessWO Borders_final.pdf).

[21] *Id.*

[22] *Id.*

[23] *Id.*