FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH 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 30, 2015

To: Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Joint Hearing on "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"

On Tuesday, November 3, 2015, at 10:00 a.m. in room 2123 of the Rayburn House Office Building, the Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology will hold a joint hearing titled "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows."

I. BACKGROUND

Generally, the United States uses a sector-by-sector approach for data protection and privacy that involves legislation, regulation, and industry self-regulation.[1] In contrast, the European Union relies in large part on comprehensive cross-sector legislation, the European Union Data Protection Directive, which sets a baseline for the required security of the storage, transmission, and processing of personal information.[2]

Data flows between the United States and Europe are the highest in the world.[3] Until recently, the flow of consumers' personal data between members of the European Union

---

[1] International Trade Administration, *U.S.-EU Safe Harbor Overview* (Dec. 18, 2013) (online at www.export.gov/safeharbor/eu/eg_main_018476.asp).

[2] *Id.*; 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).

[3] Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, Brookings Institution (Oct. 2014).

("member state") and the United States primarily was governed by an international agreement known as Safe Harbor. Safe Harbor allowed companies to move digital information, such as consumers' web search histories and social media content, between the U.S. and the European Union (EU).[4]

On October 6, 2015, the Safe Harbor agreement was ruled invalid by the Court of Justice of the European Union (CJEU), Europe's highest court.[5]

A. EU Data Protection Directive

In October 1998, the European Data Protection Directive went into effect.[6] Before its adoption, member states had widely varying approaches to the regulation of personal data processing, with some members having no rules or guidelines at all.[7]

The Directive was established by the European Commission to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of the member states, and to set a baseline of security around personal information wherever it is stored, transmitted, or processed.[8] The Directive contains basic principles for data protection, and each member state must adopt its own laws to implement those principles.[9] Each member state has adopted laws granting its citizens particular rights with respect to the processing of their personal data, and each member state is responsible for implementation and enforcement of its own laws, that implement the Directive, through "supervisory authorities."[10]

The Directive comprises 34 Articles, including provisions addressing, among other things, the rights of data subjects (defined as "an identified or identifiable natural person"), confidentiality, security, liability and sanctions, and the obligations of the independent supervisory authorities established by each member state.[11] Data protection under the Directive is primarily focused on automated data processing, in which any operation, such as collection,

---

[4] See note 1.

[5] *Data Transfer Pact Between U.S. and Europe is Ruled Invalid*, New York Times (Oct. 6, 2015) (online at www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0).

[6] *See* note 1.

[7] Rand Corporation, *Review of the European Data Protection Directive* (2009) (available at www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf).

[8] European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law* (2014).

[9] *Id.*

[10] *See* note 7.

[11] Directive 95/46/EC of the European Parliament and of the Council (Oct. 24, 1995).

storage, transmission, or destruction, is performed upon personal data by automatic means.[12] But protection also extends to manual data processing, such as paper filing.[13]

The Directive also prohibits the transfer of personal data to non-EU countries that cannot ensure an adequate level of protection for that data.[14]

B. U.S.-EU Safe Harbor Framework

Together with the European Commission, the U.S. Department of Commerce developed the U.S.-EU Safe Harbor Framework to provide a streamlined process for U.S. companies to meet the adequacy standard, which permits participating companies to transfer personal data of Europeans to U.S. servers.[15] Safe Harbor was approved by the EU in 2000, and it comprises a list of seven Safe Harbor Privacy Principles: notice, choice, transfer to third parties, access, security, data integrity, and enforcement.[16] Participation in the Safe Harbor program was voluntary, but compliance with the Principles was not.[17] It also required that participating companies annually submit a written certification of its adherence to the Principles to the Department of Commerce.[18]

A U.S. company that failed to comply with the Safe Harbor Framework after self-certifying could be subject to prosecution under state laws and Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices.[19]

II. CJEU RULING IN *SCHREMS v. DATA PROTECTION COMMISSIONER*

On October 6, 2015, the CJEU ruled that the Safe Harbor agreement is invalid concluding that U.S. law does not "ensure an adequate level of protection" of personal data, and the agreement restricted individual European nations' supervisory authorities' powers to oversee those data collection practices on behalf of their citizens.[20] The Court's decision was based on its finding that U.S. government authorities have access "on a generalized basis" to Europeans' online information.[21]

---

[12] *See* notes 7 and 11.

[13] *Id.*

[14] *See* note 11.

[15] *See* Note 1.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] Case C-362/14, *Schrems v. Data Protection Commissioner*, 2015 E.C.R. --.

[21] *Id.*

The effect of the CJEU ruling on data transfer policy and commercial behavior between the U.S. and the EU is unclear. The Article 29 Working Party, an independent advisory body made up of representatives of each member states' supervisory authorities, has said that if a new agreement between the U.S. and the EU has not been reached by January 2016, EU data protection authorities will begin taking "all necessary actions" to enforce compliance with the Directive.[22] During the transition period leading up to January, preexisting standard contractual clauses and binding corporate rules can still be used.[23] The Working Party notes, however, that transfers that are still taking place specifically under Safe Harbor are now unlawful.[24]

III. FURTHER DEVELOPMENTS

A. EU General Data Protection Regulation

In March 2015, European Commission officials announced that negotiations are nearly finished on a new set of data protection rules, known as the General Data Protection Regulation (GDPR) that would replace the European Union Data Protection Directive.[25] The GDPR will modernize data protection rules for EU member countries, addressing globalization and technological advances, such as social networking and cloud computing.[26] It will also create a more unified approach to data protection in Europe than under the current Data Protection Directive. Unlike the Data Protection Directive, the GDPR would apply directly to all EU member states without national variations, and it would not require enabling legislation to be passed by any of the states before taking effect.[27] The GDPR is set for adoption in the EU in 2017.[28]

B. New Safe Harbor Negotiations

After two years of negotiations—spurred by National Security Agency contractor Edward Snowden's disclosure of some of the U.S. government's intelligence programs—the EU and the

[22] Article 29 Working Party, *Statement on the Implementation of the Judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner Case (C-362-14)* (Oct. 10, 2015).

[23] *Id.*

[24] *Id.*

[25] *Countdown to the EU General Data Protection Regulation: 5 Steps to Prepare*, Information Age (Mar. 24, 2015) (online at www.information-age.com/it-management/risk-and-compliance/123459219/countdown-eu-general-data-protection-regulation-5-steps-prepare).

[26] *Id.*

[27] *Id.*

[28] *Id.*

U.S. have reportedly agreed on a new data transfer pact in principle.[29] Many observers are unsure whether a new agreement will withstand legal challenges.[30]

The terms of this new agreement have not been shared publicly. However, it is expected to address, among other things, increased oversight by the Department of Commerce, redress mechanisms for consumers who feel that their data has been mishandled, and an annual review mechanism that would monitor whether law enforcement and national security services have complied with limits on access to European's data.[31]

C. H.R.1428, the Judicial Redress Act of 2015

On October 20, 2015, the House passed the Judicial Redress Act of 2015. The bill authorizes the Department of Justice to designate foreign countries whose citizens may bring civil actions against certain U.S. government agencies under the Privacy Act of 1974 if their personal information is mishandled by federal agencies that received it for the purposes of preventing, investigating, detecting, or prosecuting criminal offenses. A foreign country will only qualify for designation under the Act if it has appropriate policies on sharing information relating to criminal investigations with U.S. law enforcement.

IV. WITNESSES

The following witnesses have been invited to testify:

John Murphy
Senior Vice President for International Policy
U.S. Chamber of Commerce

Victoria Espinel
President and CEO
BSA/The Software Alliance

Joshua Meltzer
Senior Fellow
Brookings Institution

Marc Rotenberg
President and Executive Director
Electric Privacy Information Center

---

[29] *EU, U.S. Agree in Principle on New Data-Transfer Pact*, Wall Street Journal (Oct. 26, 2015) (online at www.wsj.com/articles/eu-u-s-agree-in-principle-on-data-pact-1445889819?mod=WSJ_TechWSJD_NeedToKnow).

[30] *Id.*

[31] *Id.*