U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

October 30, 2015

TO: Members, Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology

FROM: Committee Majority Staff

RE: Joint Hearing entitled "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows."

I. INTRODUCTION

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

II. WITNESSES

The Subcommittees will hear from the following witnesses:

- Victoria Espinel, President and CEO, Business Software Alliance;
- Joshua Meltzer, Senior Fellow, Global Economy and Development, The Brookings Institution;
- John Murphy, Senior Vice President for International Policy, U.S. Chamber of Commerce; and
- Marc Rotenberg, President, Electronic Privacy Information Center.

III. BACKGROUND

Global cross-border data flows have become an essential component of all international companies' daily operations and have supported tremendous innovation and growth across multiple industries. The infrastructure supporting these data flows also support local businesses and jobs. Businesses are able to harness economies of scale to provide goods and services to their clients and customers in the most efficient manner because of the free flow of data. The U.S. and European Union (EU) are the largest trading markets in the world. The bilateral trade relationship between the U.S. and the 27-member EU is the world's largest with the two

economies combined accounting for forty percent of world output and over $1 trillion in trade.[1] The economic impact of cross border data flows will only increase as usage of and reliance on the Internet increases across the world. This strong trade relationship dovetails with other aspects of the strong relationship between the U.S. and the EU.

The 2000-2015 U.S.-EU Safe Harbor Framework Principles

The U.S.-EU Safe Harbor Framework (Safe Harbor or SHF) was developed shortly after the European Commission's Directive on Data Protection was enacted in 1998 to allow for interoperability between the different approaches the U.S. and European Union have implemented to address commercial data privacy and allow the free flow of data.[2] The Safe Harbor required U.S. companies to self-certify compliance with the Department of Commerce by either joining a self-regulatory program that adheres to the Safe Harbor requirements or develop its own program to comply with the seven principles in order to legally transmit data about EU citizens outside of the EU.[3] Self-certifications were subject to initial and annual review by the Department of Commerce with enforcement actively managed by the Federal Trade Commission (FTC).[4] The FTC enforces the Safe Harbor through the same section 5 authority that it has used to bring over fifty data security enforcement actions.[5] The FTC's enforcement regime compliments the over 300 state and federal laws governing data privacy.

As of October 2014, there were over 4,400 businesses self-certifying compliance with the Safe Harbor.[6]

The seven principles of the Safe Harbor:

1. **Notice** – Companies must notify individuals about why they are collecting and using information about them, provide contact information for questions or complaints, and disclose the types of third parties that have access to the data and what choices the individual has for limiting its use and disclosure.

2. **Choice** – Individuals must have an opt-out choice for whether the personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for the original collection. For sensitive information, individuals must opt-in if the information is disclosed to a third party or used for a purpose beyond which it was originally collected.

---

[1] http://www.ustr.gov/countries-regions/europe-middle-east/europe/european-union, http://useu.usmission.gov/economic_issues.html.
[2] http://export.gov/safeharbor/eu/index.asp
[3] http://export.gov/safeharbor/eu/eg_main_018476.asp
[4] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework
[5] Testimony of Jessica Rich, Director of the Bureau of Consumer Protection, Federal Trade Commission, before the Subcommittee on Commerce, Manufacturing, and Trade (March 18, 2014), http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-RichJ-20150318.pdf..
[6] https://safeharbor.export.gov/list.aspx

3. **Transfers to Third Parties** – In order to share information with a third party, companies must either make sure that the third party subscribes to the SHF or contract directly with the third party requiring them to provide at least the same level of privacy protection as required by the SHF.

4. **Access** – Individuals must be able to access, correct, amend, or delete personal information that the company has about them where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy or where the rights of another individual would be violated.

5. **Security** – Companies must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alternation, and destruction.

6. **Data integrity** - Personal information must be relevant for the purposes for which it is to be used. A company should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

7. **Enforcement** - There must be (a) readily available and affordable independent recourse mechanisms so that each complaint and dispute can be investigated and resolved and damages awarded, (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented,[7] and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization.

While it is possible to comply with the Directive on Data Protection through EU-approved standard contractual clauses (SCCs or model contract clauses) or binding corporate rules (BCRs), these mechanisms are not available to every business, impose a significant cost, and involve a lengthy approval process that can range from a few months to several years.

Legal Challenges and Renegotiation of the Safe Harbor Framework post-Snowden

In November 2013, the European Commission (EC) released a series of 13 recommendations to update the Safe Harbor framework as a response to "deep concerns about revelations of large-scale U.S. intelligence collection programmes."[8] The U.S. Department of Commerce and their ECcounterparts began renegotiating the Safe Harbor in early 2014.

---

[7] In January 2014, the FTC settled with 12 U.S. companies falsely claiming to comply with the Safe Harbor Framework. https://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply. *See also* "Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework (Nov. 12, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf.

[8] "Restoring Trust in EU-US data flows – Frequently Asked Questions," European Commission – Memo/13/1059. November 27, 2013. http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm. *See* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

The 13 recommendations from the European Commission to update the Safe Harbor are:[9]

Transparency

1. Privacy policies should be publically posted on companies' websites in clear and conspicuous language. It is not sufficient for companies to provide the Department of Commerce with a description of their privacy policy.

2. Privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbor website, which lists all the "current" members of the scheme. Since March 2013, the Department of Commerce has requested this from companies, but the process should be intensified.

3. Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services. Safe Harbor allows onward transfers from Safe Harbor self-certified companies to third parties acting as "agents," for example to cloud service providers by contract that provides at least the protection of the Safe Harbor. When entering such a contract, a Safe Harbor company should also notify the Department of Commerce and make the privacy safeguards public.

4. Clearly flag on the website of the Department of Commerce all companies that are not current members of the scheme. However, in the case of "Not current," the company is obliged to continue to apply the Safe Harbor requirements for the data that has been received under Safe Harbor.

Redress

5. The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider and/or EU panel. This will allow European data subjects to contact the ADR or EU panel in case of problems. Since March 2013, Department of Commerce has requested this from companies, but the process should be intensified.

6. ADR should be readily available and affordable. Some ADR bodies in the Safe Harbor scheme continue to charge fees from individuals – which can be quite costly for an individual user – for handling the complaint ($200-250). By contrast, in Europe, access to the Data Protection Panel to solve complaints under the Safe Harbor is free.

7. The Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.

Enforcement

8. Following the certification or recertification of companies under the Safe Harbor, a certain percentage of these companies should be subject to ex officio investigations of

[9] http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

effective compliance of their privacy policies (going beyond control of compliance with formal requirements).

9. Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after one year.

10. In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority.

11. False claims of Safe Harbor adherence should continue to be investigated.

Access by US authorities

12. Privacy policies of self-certified companies should include information on the extent to which U.S. law allows public authorities to collect and process data transferred under the Safe Harbor.

13. It is important that the national security exception foreseen by the Safe Harbor Decision is used only to an extent that is strictly necessary or proportionate.

Notwithstanding the in-progress renegotiation of the Safe Harbor, on October 6, 2015, the Court of Justice of the European Union (ECJ) ruled that the U.S.–EU Safe Harbor Framework is no longer available as a valid transfer mechanism for data between the U.S. and the EU.[10] The ECJ ruled to overturn the European Commission Decision 2000/520/EC (July 26, 2000) pursuant to Directive 95/46 that had previously deemed transfers through the Safe Harbor as "adequate" to fulfill the data protection requirements of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Charter).[11] While there are a variety of differences between the U.S. legal system and the EU legal system that are important when reviewing the decision, the result of the decision is not in dispute and has created a substantial amount of uncertainty for businesses conducting transatlantic business.

The Article 29 Data Protection Working Party (Article 29 Working Party), established by Directive 95/46/EC, is an independent advisory group comprised of representatives from each EU country. After the ECJ's decision removing the Safe Harbor as a valid data transfer mechanism, the Article 29 Working Party issued a statement indicating that negotiators have until the end of January 2016 to find a path forward before each EU country's data protection authorities may proceed with independent or coordinated investigations into companies

[10] On June 25, 2013, Mr. Schrems filed a complaint with the Irish Data Protection Commissioner (DPC) claiming that the laws of the U.S. offer no real protection against State surveillance following the Snowden revelations regarding intelligence services' access to data. The ECJ's decision earlier this year was a preliminary ruling on the validity of Decision 2000/520 request by the Irish High Court on appeal of the Irish DPC's dismissal of Schrems' claim as "frivolous or vexatious." Maximillian Schrems v. Data Protection Commissioner, C-362/14 (Final Decision, October 6, 2015), http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN.
[11] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

transferring data.[12] The final paragraph of the statement states that "businesses should reflect on the eventual risks they take when transferring data and should consider putting in place any legal and technical solutions in a timely manner to mitigate those risks and respect the EU law protection [laws]."[13]

U.S. Law Revisions post-Snowden

On June 2, 2015, President Obama signed the USA Freedom Act into law after bipartisan votes in both the House of Representatives and the Senate.[14] The USA Freedom Act was a major reform of U.S. surveillance law that increased civil liberties protections by ending bulk collection of records and strengthened challenge procedures and review requirements for national security letter gag orders.

Presidential Policy Directive/PPD-28[15] was signed by President Obama on January 17, 2014, and clarified the limited scope of signals intelligence collection activities while highlighting the importance of privacy and civil liberties.[16]

On October 20, 2015, the House of Representatives passed the bipartisan Judicial Redress Act, H.R. 1428, by voice vote. H.R. 1428, which authorizes the Department of Justice to designate countries or regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records maintained by an agency.[17] Senator Hatch and Senator Murphy introduced a companion bill, S. 1600, which has been referred to the Judiciary Committee for consideration.

Next Steps

The Department of Commerce is continuing negotiations with the European Commission on a new data transfer agreement.[18] The Department of Commerce has included an advisory on its Safe Harbor websites notifying companies that "[i]n the current rapidly changing environment, the Department of Commerce will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework. If you have questions, please contact the European Commission, the appropriate European national data protection authority, or legal counsel."[19]

---

[12] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf
[13] *Id.*
[14] http://judiciary.house.gov/index.cfm/usa-freedom-act
[15] https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf
[16] https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities
[17] http://www.msnbc.com/msnbc/nsa-reform-compromise-clears-house-hurdle
[18] Briefing with the Department of Commerce staff, October 27, 2015.
[19] https://safeharbor.export.gov/list.aspx

Reports indicate progress is being made on negotiations.[20] European Justice Commissioner Vera Jourova stated earlier this week that the U.S. and EU have reached an agreement on principles and expects "significant progress" on the outstanding technical points by her visit to the U.S. in mid-November.[21] With the impending January 2016 deadline indicated by the Article 29 Working Party, the timeline to reach a new agreement is compressed for negotiators and companies.

IV. ISSUES

The following issues may be examined at the hearing:

- What is the immediate impact on U.S. industry following the European Court of Justice's decision in the *Schrems* case?
- How has the uncertainty following the Court of Justice's decision impacted small and medium businesses that conduct transatlantic business?
- What industries outside of the technology sector are impacted by the *Schrems* ruling?
- What steps are businesses taking to evaluate the risk they face in light of the January 31, 2016 deadline announced by the Article 29 Working Group? Are there particular concerns for small and medium businesses?
- What would it mean for the global economy if certainty is not restored for U.S. companies doing business with customers and consumers in the European Union?

V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Paul Nagle, David Redl, Grace Koh, or Melissa Froelich of the Committee staff at (202) 225-2927.

[20] Last week at the Coalition of Services Industries' annual summit meeting, Secretary Pritzker said that the U.S. and EU had "a handshake" on a new Safe Harbor agreement earlier in the year but the European Commission's negotiators "were not willing to release it." Briefing with Department of Commerce staff.
[21] Natalia Drozdiak, "EU, U.S. Agree in Principle on New Data-Transfer Pact" *Wall Street Journal*, October 26, 2015 (last accessed October 29, 2015) http://www.wsj.com/article_email/eu-u-s-agree-in-principle-on-data-pact-1445889819-lMyQjAxMTE1MzIyNzAyMTc5Wj.