Testimony of
Edward M. Dean, Deputy Assistant Secretary for Services,
International Trade Administration, U.S. Department of Commerce
Before the House Energy and Commerce Subcommittees on Commerce,
Manufacturing and Trade and Communications & Technology
U.S.-EU Safe Harbor Framework
November 3, 2015

I. Introduction

Good Morning, Chairmen Burgess and Walden, Ranking Members Schakowsky and Eshoo and distinguished Committee Members. Thank you for the opportunity to submit written testimony about the U.S.-EU Safe Harbor Framework. I have welcomed the high-level attention Committee Members have brought to Safe Harbor since the October 6 European Court of Justice (ECJ) decision. Your statements, letters and outreach have highlighted the importance of Safe Harbor to U.S.-EU trade and the need to promptly endorse the strengthened Framework that we have negotiated with the European Commission during the past two years. With over 4,400 companies in the United States utilizing the program, it is a cornerstone of the transatlantic digital economy enabling growth and innovation in the United States and in Europe. As a result, it is my top priority and is a top priority of our Secretary of Commerce and the Administration as a whole.

In my capacity as Deputy Assistant Secretary for Services in the International Trade Administration, I oversee the team administering the Safe Harbor Framework at the Department of Commerce and have led our consultations with the European Commission over the past two years to update Safe Harbor. In this testimony, I will provide a brief history of the Safe Harbor Framework and our engagement with the European Commission. I will then discuss the ECJ decision, its implications and our work to ensure data flows between the United States and EU can continue.

II. History of the U.S.-EU Safe Harbor Framework

The Safe Harbor Framework has, for 15 years, served as a model for the protection of privacy while facilitating data flows that fueled growth and innovation on both sides of the Atlantic. Safe Harbor was developed by the U.S. Department of Commerce and European Commission following the adoption in 1995 of the EU Directive on Data Protection (EU Directive 95/46/EC). The EU Directive came into effect in 1998, restricting the transfer of personal data to non-EU countries that did not meet the EU "adequacy" standard for privacy protection. While the United States and the EU share the goal of protecting the privacy of our citizens, the U.S. approach to privacy, which includes sectoral privacy legislation, state laws, and robust enforcement by the U.S. Federal Trade Commission, has not been deemed adequate by the EU.

In order to bridge these differences in approach and provide a means for U.S.-based companies to receive data from the EU in compliance with the EU Directive, the U.S. Department of Commerce in consultation with the European Commission developed the Safe Harbor Framework. The Safe Harbor Framework was designed as a voluntary, enforceable code of

conduct based on globally-recognized privacy principles to which U.S.-based companies could self-certify. Under Safe Harbor, U.S.-based companies voluntarily certify their commitments to Safe Harbor's data protection requirements. In doing so, those companies' public commitments and attestations became enforceable by the U.S. Federal Trade Commission. The Safe Harbor Framework was deemed "adequate" by the European Commission and EU Member States in 2000. The Department of Commerce has worked closely with the European Commission since the program's inception to strengthen the operation of program within the parameters of the existing Framework.

By the time of the European Court of Justice ruling, over 4,400 companies in the United States were participating in Safe Harbor and relying on the European Commission's determination that it provided adequate protection to process data in the course of transatlantic business. These 4,400 participants come from nearly every sector of the economy. 61% of the companies are small and medium sized businesses with 250 or fewer employees. They include U.S.-headquartered companies, as well as U.S.-based subsidiaries of EU companies. While media focus has centered on data exchanged through social networks and as part of cloud services, Safe Harbor participants process a wide variety of data from Europe to conduct business. This includes human resources data of EU-based employees, shipping and billing information for the purchase of goods and services, and transactional data necessary to support 24/7 customer service. In short, the global trading and financial system today depends on the ability to seamlessly send and receive personal data without regard for national borders. This dependence is revealed by the more than $240 billion worth of digitally deliverable services trade between the United States and Europe. Safe Harbor ensured that this data could move both efficiently and in compliance with EU law.

III. Recent Developments and DoC Engagement

Following the surveillance disclosures in 2013, the European Parliament and some EU Member State officials called for suspension of the Safe Harbor Framework. The European Commission responded with a review of the Framework followed by the release of a Communication with 13 recommendations to improve the Framework. The first eleven related to commercial data flows and the last two pertained to national security issues. Following the release of the Commission's Communication in November 2013, the Department of Commerce initiated consultations with the Commission to address their recommendations.

Before describing the negotiations, it is worth saying a few words about the broader political context in Europe around these issues. Since Safe Harbor had become linked to the surveillance disclosures, it became a target for continued criticism largely based on misunderstanding and false assumptions about its purpose and operation and the important privacy benefits it provided. At their heart, many of these criticisms were based on false accusations that the United States was engaged in "mass, indiscriminate surveillance" of the data transferred to the United States under Safe Harbor.

For the past two years, the Department, along with the U.S. Federal Trade Commission and Department of State, has engaged in consultations with the European Commission. We have also worked with officials from the Intelligence Community and the Department of Justice to discuss the national security-related recommendations. Recognizing the importance of data

flows and the challenging political context in which we were operating, we worked hard to strengthen the framework and address concerns raised in the EU. In our view, it was appropriate to modernize the 15-year old Framework, and there were improvements and changes we could make that enhanced privacy protections while continuing to facilitate data flows. Throughout this process, we consulted regularly with U.S. stakeholders to discuss both the privacy benefits and commercial feasibility of potential changes. We were mindful of areas that might cause new compliance costs for U.S. firms and pushed back in our negotiation when we felt that any change might unduly burden U.S. firms relative to other companies. These were difficult negotiations, but over the summer we reached a tentative agreement that was subject to review and approval by the European Commission's political leadership. At that point, the Commission chose not to move forward given the pending issuance of the European Court of Justice Decision.

In its October 6 ruling, the European Court of Justice invalidated the European Commission's determination in 2000 that Safe Harbor provides adequate protection for personal data. This determination by the Commission was the legal foundation for Safe Harbor. The ECJ decision did not examine or make findings regarding the adequacy of U.S. protections; rather, it faulted the European Commission for examining Safe Harbor but not the broader U.S. legal context in 2000. Unfortunately, the ECJ decision did not allow a transition period for companies to make alternate legal arrangements, creating even greater legal uncertainty.

We are deeply disappointed in the ECJ decision, which creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy. The ruling does not give adequate credit for the robust protections of privacy available in the U.S. or all that the Framework has done to protect privacy and enable economic growth. We are focused on and fully committed to resolving the uncertainty that the decision has created and thus end the significant, negative consequences that flow from such uncertainty.

We fully understand how harmful uncertainty can be to a business, its growth, employees, customers, and vendors, and have been hearing directly from companies, large and small, about the real world impact of the ECJ decision. We have stressed to the Commission that real harm is presently being borne by companies that have committed in good faith to protect privacy in accordance with globally recognized principles. It is worth emphasizing that the ECJ decision does not question whether U.S. companies provided their consumers with the protections promised under the Safe Harbor.

To illustrate just how harmful the uncertainty created by the ECJ decision has been, I offer two illustrative examples:

- A small company, which provides support services relevant to clinical research trials, has already lost significant business across Europe. The company's clients are suspending and shutting down projects, while its EU-based main competitor has reached out to other existing clients recommending they switch providers in light of the court ruling.

- A large U.S.-based hotel chain with properties across the EU would in the absence of Safe Harbor have to either: put in place EU model contracts with each of its vendors –

something it described as a logistical nightmare – ; or, take on the EU's binding corporate rules process, which is very expensive and has an 18-month lead time.

While model contracts, binding corporate rules, and other options for compliance with European privacy law do exist, the ECJ ruling has also raised questions about their viability. For example, following the ECJ ruling, a German DPA released a position paper indicating that model contracts and consent might also be considered invalid for transferring data to the United States.

We believe the best way to protect privacy and restore confidence in transatlantic data flows is to promptly endorse and put in place the strengthened Safe Harbor Framework that we have negotiated with the European Commission during the last two years. We have provided a very strong basis for the European Commission to make the findings discussed in the ECJ decision, including on the national security issues. That being said, we are continuing to discuss ways to improve and strengthen the overall package now, and to be sure that it addresses the specific issues raised by the court.

This is a priority for me, for Secretary Pritzker and for the Administration as a whole. We have welcomed many of your own calls for this important step. Secretary Pritzker, senior officials at the White House and across the interagency community have been in close and regular contact with the European Commission, as well as other partners across Europe, including within individual Member States, and have expressed the need for urgent resolution of this issue. I was in Europe during each of the past three weeks meeting with the European Commission, EU data protection authorities, EU Member State officials and affected U.S. and EU businesses to discuss the path forward. Our Secretary, Deputy Secretary, and the Under Secretary for International Trade among other senior officials have also traveled to Europe during this time. Each has engaged on this issue both during their trip as well as from Washington.

IV. Conclusion

We remain committed to doing everything we can, as fast as possible, to move forward with a new Safe Harbor Framework. We are prepared to focus full time on this issue in order to bring greater certainty around the critical issue of data flows. We are hopeful that our partners in the Commission will be willing to approach this with the same sense of urgency, and we appreciate the focus you and your colleagues here in Congress can bring to this important issue.