Testimony of
Nicole Y. Lamb-Hale, Assistant Secretary for Manufacturing and Services,
International Trade Administration, U.S. Department of Commerce
Before the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade
Internet Privacy: The Impact and Burden of EU Regulation
September 15, 2011

I. Introduction.

Good Morning, Madame Chair Bono Mack, Ranking Member Butterfield, and distinguished Committee Members, thank you for the opportunity to testify about online privacy and the impact the European Union's (EU) legal framework for data protection has on U.S. companies doing business in one or more of the EU member states. My testimony is particularly timely in light of the fact that the Department's Internet Policy Task Force has received feedback from industry and consumers that an enhanced U.S. privacy framework would facilitate mutual recognition of commercial data privacy laws around the world, thereby increasing practical protection for consumers and the reduction of barriers and compliance costs for U.S. companies in international markets.[1] In my capacity as the Assistant Secretary for Manufacturing and Services in the International Trade Administration, I will outline the approaches taken by the EU and the United States with respect to commercial data protection, describe the impact that the EU framework has on U.S. companies, and explain what the United States, in particular, the U.S. Department of Commerce (Department) is doing to facilitate unencumbered transatlantic trade.

II. The European Union and United States' legal regimes for data protection and privacy

The EU and the United States share common goals in desiring to protect individuals' privacy while pursuing economic growth through increased trade and investment and by supporting Internet innovation. We arrived at these shared goals through over thirty years of transatlantic dialogue, beginning in the 1970s with the enactment of early data privacy laws in the US, Europe, and other democracies around the world. Our understanding and implementation of these common principles is influenced, however, by different historical perspectives and underlying differences in regulatory philosophy of our legal systems. Both these similarities and differences have influenced the developments of our respective data privacy legal frameworks.

EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, otherwise known as the EU Data Protection Directive, was issued by the European Parliament and the EU Council in 1995, and is currently under review. The Directive is drawn in part from the 1980 Organization for Economic

[1] All comments received by the Department in response to its Notice of Inquiry on the impact of privacy laws on innovation are available at http://www.ntia.doc.gov/federal-register-notices/2010/information-privacy-and-innovation-internet-economy-notice.

Cooperation and Development Guidelines (OECD Guidelines) on the Protection of Privacy and Transborder Data flows of Personal Data, which was endorsed by the United States and other OECD member countries, and provides a shared foundational understanding of key commercial data privacy rights and obligations among OECD countries. In the EU, the protection of personal data is included in the Charter of Fundamental Rights and the EU Data Protection Directive (EU Directive) provides the legal basis for protection of European citizens' personal data and privacy upon which national laws of the EU member states have been enacted. The EU Directive functions as a baseline for EU member states and allows them to adopt more stringent national protections. Additionally, Directive 2002/58 on Privacy and Electronic Communications, otherwise known as the E-Privacy Directive, complements the EU Directive, focusing specifically on protecting the privacy of Europeans active in the online environment. The EU amended this directive in 2009 to add requirements related to security breaches, spyware, cookies, and spam.

In the United States, the protection of individual privacy is deeply embedded in law and policy. The current legal framework consists of constitutional rights, common law, consumer protection statutes, and sector-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Electronic Communications Privacy Act (ECPA). The various laws are enforced by the states, the courts, and by federal agencies such as the Federal Trade Commission (FTC). Voluntary multi-stakeholder policy development complements this framework.

This framework has encouraged innovation and provided many effective privacy protections. Focused civil and criminal law enforcement is applied when intervention is necessary to mitigate harm to the consumer. In particular, the FTC has been enforcing certain online consumer privacy protection through Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. The states have additional consumer protection statutes. Supplementing this legal framework and government enforcement is a mix of self-regulating oversight organizations, trustmark seal programs, and codes of conduct. But certain key American players in the Internet, including online advertisers, cloud computing service providers, providers of location-based services, and social networking sites, operate in sectors without specific statutory obligations to protect information about individuals. Because of this, and as Assistant Secretary Strickling noted in his testimony before this Committee on July 14th, the Administration is advocating for stronger consumer protection in the on-line environment.

III. How U.S. Companies Navigate EU's Privacy Framework

In the international context, the EU Directive imposes limitations on cross border data flows to countries whose legal frameworks do not meet its adequacy requirements as determined by the European Commission (EC), the executive arm of the EU. In 1998, the Department embarked on a two-year negotiating process with the EC aimed at devising ways for U.S. companies to continue doing business with firms in the EU without unnecessarily burdensome obligations being imposed on their activities. The result was the U.S.-EU Safe Harbor Framework (Safe Harbor Framework), a policy approach that the EC deemed adequate in a July 26, 2000 finding. The Framework remains in force today.

The U.S.-EU Safe Harbor Framework went into effect on November 1, 2000. It is administered by the Department's International Trade Administration (ITA) on behalf of the United States. The Safe Harbor Framework is comprised of seven privacy principles, modeled on the OECD Guidelines and the EU Directive, as well as 15 FAQs that provide explanatory guidance to interested parties. The Safe Harbor Framework is a voluntary arrangement under which U.S. commercial entities may seek to undertake to comply with the framework principles and publicly declare they will do so. The Department maintains a website that provides a wealth of information to the business community on the elements of the program, the application process, renewal, and links to the EU's data protection unit under the Directorate General for Justice (DG Justice), the oversight authority in the EC. It also maintains a list of those U.S. firms that have self-certified their adherence to the Safe Harbor principles.

When the Safe Harbor Framework was launched, four companies self-certified their compliance to the program. Today, nearly 3,000 companies of all sizes belong, and we add more than 60 new members each month. This service has enabled small and medium-sized enterprises to provide a range of value-added products and services to EU clients and citizens without the expense of hiring European legal counsel to comply directly with the EU's legal framework. Onward data transfers are covered by the Safe Harbor Framework's onward transfer principle and allow organizations to move data to secondary processors. An estimated half trillion dollars in transatlantic trade is facilitated by the Safe Harbor Framework.

We have received assurances from the EC that the Safe Harbor Framework will continue to be a viable option for U.S. companies even as the EU revises its Directive. The Safe Harbor Framework is important to U.S. companies and their EU partners who rely on U.S. information technology service providers to provide state-of-the art products to their customers. The advent of cloud computing services in the EU presents its own set of challenges and we work regularly with our counterparts in the EC and at the member state level to clarify how personal data is protected in the "cloud."

Some large U.S. multinational corporations have chosen to avail themselves of alternative means of complying with the Directive, but these have proven to be costly and time-consuming. For example, several large U.S.-based multinational corporations have chosen to use binding corporate rules (BCRs), which permit global intra-corporate data flows if the corporation's practices for collecting, using, and protecting that data are approved by the data protection authorities in the EU. Despite recent efforts to streamline the approval process, the costs and time associated with obtaining approval of the BCRs are substantial. That may be why only very large multinational corporations use BCRs to comply with EU data protection laws.

Generally speaking, the biggest problems U.S. companies face with regard to navigating the privacy landscape in Europe include: 1) the significant resources that must be allocated to comply with these regulations (if they are not in Safe Harbor); 2) several EU member states implement the EU Directive differently so U.S. firms must comply with a variety of requirements in as many as 27 member states; and, 3) the differing EU member state regulations create legal uncertainty which complicates U.S. companies' efforts to plan for

the future. In addition, several U.S. companies – including cloud computing and social networking companies – have faced numerous challenges in the EU with regard to their business models and their privacy practices. Some of these challenges are a result of confusing requirements in the various member states.

IV. How the Department of Commerce Is Working Toward Greater Interoperability with the EU Privacy Framework

During testimony given at March and June hearings of the United States Senate Committee on Commerce, Science, and Transportation, my colleagues from the Department announced the Administration's support for legislation that would create baseline consumer data privacy protections through a "consumer privacy bill of rights." The Administration has been developing its views in more detail in a "White Paper" on consumer data privacy, which we hope to finalize this fall. One of the important concepts included in this paper is the need for greater interoperability of global commercial data privacy regimes.

While the Safe Harbor Framework has proven itself to be valuable in facilitating transatlantic trade, it is not a perfect solution for all U.S. entities. Sectors not regulated by the FTC, such as financial services, telecommunications, and insurance are not covered by the framework because their regulators were not part of the negotiations. Some companies in these sectors have indicated that they would like to see an improved environment for transatlantic data transfers.

The Department continues to engage the EU and its member states in discussions on how we can facilitate commercial data flows while at the same time respecting each other's laws and values. As Assistant Secretary Strickling noted in his testimony before this Committee on July 14, the Department has engaged in extensive conversations with EU data protection officials at all levels during the more than 10 years since the EU Directive entered into force. We have frequently engaged with senior officials from the EC, the European Data Protection Supervisor, members of the European Parliament, and national data protection commissioners. These interactions have been designed to convey to the EU that the U.S. legal framework, albeit structured differently, is as robust as the EU's framework for protecting individuals' privacy.

To build on the success of the Safe Harbor Framework, we hope to develop additional mechanisms that support mutual recognition of legal regimes, facilitate the free flow of information, and address emerging challenges. Specifically, we are considering the establishment of a multi-stakeholder process to produce enforceable codes of conduct that companies would then choose to adopt. In an open forum convened by the government, stakeholders with an interest in a specific market or business context will work toward consensus on a legally enforceable code of conduct that implements the Consumer Privacy Bill of Rights and other protections as appropriate. Under our proposed privacy framework, codes of conduct developed through this process would be enforced by the FTC, a world-leading privacy and consumer protection enforcement authority.

We in the Department believe that well-crafted multi-stakeholder consultation processes for Internet policy making are essential because they can nimbly respond to new challenges,

which in turn fosters confidence and clarity for consumers, industry, and other stakeholders. The attributes of speed, flexibility and decentralized problem-solving promoted by such multi-stakeholder consultations offer many advantages over traditional government rulemaking when it comes to establishing rules and guidelines that promote innovation and effectively protect consumers.

It is for this reason that the Administration supports a three-part legislative framework for consumer data privacy that includes principles-based privacy protections in the commercial sectors that are not subject to existing Federal data privacy statutes, encouragement for codes of conduct developed through a multi-stakeholder approach, and enhanced consumer data privacy enforcement authority for the FTC. The challenge is to find a way forward that allows this dynamic and stakeholder-driven process to reduce barriers to cross border data flow, but that is based on enhanced protections. We hope to include European stakeholders in our multi-stakeholder processes. While differences between the U.S. and EU commercial data privacy framework exist, our goals remain congruent. We both seek to protect individual consumers' personal information while promoting the appropriate free flow of information and global trade.

V. Conclusion

Thank you for the opportunity to explain how the EU's privacy and data protection framework relates to the commercial interests of the United States, to explain what the Department of Commerce is doing to help U.S. companies navigate privacy regulations in the EU, and to promote a legislative framework for consumer data privacy that continues to protect their privacy without stifling innovation and trade.