U.S. CHAMBER OF COMMERCE

BUSINESSEUROPE

May 4, 2017

The Honorable Wilbur Ross
Secretary
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Mr. Andrus Ansip
Vice President
European Commission
Rue de la Loi 200
B – 1049 Brussels

Dear Secretary Ross and Vice President Ansip,

The U.S. Chamber of Commerce and BusinessEurope represent the interests of American and European businesses of every size and sector as well as of local chambers and industry associations. We are steadfast supporters of the transatlantic alliance and its benefits to American and European workers, consumers, and companies. These benefits are increasingly reliant on the integration of technology in virtually all aspects of the transatlantic economy.

Thanks to the innovation and productivity of American and European companies, the United States and European Union have become the leaders of the global digital economy, which generates over $8 trillion / €7.4 trillion a year. It is critical that our regulatory regimes promote policies that continue to foster our digital economies across the Atlantic and globally. Today, we write to you with a number of recommendations that will further encourage innovation to drive transatlantic leadership, economic growth and prosperity.

**Reaffirm Commitment to the U.S.-EU Privacy Shield Framework**

First, we believe that it is vitally important to build upon the achievements of the U.S.-EU Privacy Shield Framework and the commitments made by the United States and the EU that underpin its implementation. A clear affirmation by both sides following the first annual review in September is essential. American and European companies rely on the legal certainty provided by the framework to transfer data and export digital goods and services. The Privacy Shield reiterates the U.S. and EU governments' commitment to a transatlantic digital economy that keeps data protected while enabling commercial data flows that are critical to economic growth.

Privacy safeguards managing the movement of data are understandably important but need not hinder economic growth. The transatlantic marketplace will thrive under privacy regimes that promote trade and foster consumer trust in the cloud and data-driven technologies. The United States and EU should foster effective and modern data protection governance systems. The EU is carrying this out through the creation of regulatory Guidelines to aid application of its new General Data Protection Regulation (GDPR) in the Digital Single Market. It has also proposed a new ePrivacy Regulation. In an increasingly data-driven economy, policymakers must work with the private sector in order to understand and adapt to the evolving technology and business landscape. These efforts should be pursued in ways that encourage innovation and creativity, support digital trade, and recognize that differing approaches to these issues can achieve compatible outcomes.

**Foster Cross-Border Data Flows and Eliminate Unjustified Data Localisation**

Second, the question of local data requirements needs urgent attention. Data is at the heart of the digital economy. Ninety percent of the data that exists today did not exist two years ago. At this pace, it is expected that data will grow at a rate of more than 200% a year. Everyone recognizes capital flows are critical to the American, European and global economy. Increasingly, data flows are on par with the importance of the movement of goods, services, and capital. Businesses on both sides of the Atlantic are leveraging the digital economy to grow in new ways. In fact, cross-border data flows between the United States and Europe are the highest in the world, and our economies have used data flows to achieve a combined digital trade surplus of over $310 billion. In the past decade, data flows have raised global GDP by 10%. But this is at risk of slowing just when the possibilities offered by data are speeding up.

National data localization requirements force certain types of data to remain in certain territories. Not only is this highly costly and a drain on innovation, but it has no security merit as businesses would be deprived of the ability to deploy best technical practices and store data in a single location. Businesses need to move data to create worth. In order to capture the full benefits of transatlantic data flows for our economies and society, the United States and EU must eliminate current and prevent future forced data localisation requirements. Further, they must work together reduce the forced localization of data storage around the world. When impediments to the digital economy such as data localization are eliminated around the world, the EU and the United States are better-prepared than any other economies to benefit from open digital markets.

**Avoid Data "Ownership", Access and Liability Rules that Inhibit Innovation**

Third, it is essential that rules surrounding current emerging data issues not impede innovation. While a legal concept of data ownership does not exist in practice, contractual agreements are made that enable flexible uses of data while ensuring parties involved understand their ownership rights. Setting entirely new or untested concepts could lead to

unforeseen consequences. This is also true regarding third party data access. A variety of conflicting commercial interests such as investment, competition and IP mean that no two situations of data access are the same. Therefore, blanket rules for data access would be damaging. Continuing contractual law practices for commercial transfers of personal and non-personal data allow for adaptation to the situation at hand.

We recognize that new technologies are creating multiple interdependencies between products and service developers; this might raise questions around liability. Yet this is not entirely new as many complex supply and value chains already exist in more tangible sectors, and questions regarding liability are already sufficiently answered through existing product liability law.

**Apply Collaborative, Market-Based Solutions to Cybersecurity**

Fifth, approaches to security must remain collaborative, flexible, and innovative over the long term—enabling solutions to evolve at the pace of the market. Overly prescriptive, burdensome, one-size-fits-all cybersecurity rules must be avoided. The United States and EU have both created cybersecurity frameworks that encourage public-private partnerships, information sharing, and risk management approaches to tackling security challenges. Further cooperation is necessary to fully understand how the EU's NIS Directive and the U.S. NIST Cybersecurity Framework complement one another. This understanding will allow companies to easily align with both frameworks, therefore strengthening the security of the transatlantic digital economy. Continued collaboration between government and industry is critical and global standards bodies should remain actively engaged.

**Promote the Development of Industry-Driven Standards in Global Fora**

Sixth, standardization is an important element in building and sustaining digital leadership. Standards based on market incentives and investment programs foster innovative solutions and growth. Development of standards is best suited to take place globally through standardization development organizations and consortia.

These vehicles produce globally recognized, voluntary, industry-driven standards that enable interoperability to fit various technologies together. Standardizers recognize the importance of coordinating and cooperating initiatives in these global consortia/fora. The United States and EU must continue to promote these vehicles for standards development, particularly with the increasing push for top-down government driven initiatives in other regions.

**Adopt a Holistic View of the Internet of Things**

Finally, as more traditional products and services connect and depend on data to function, it is important that a holistic view is adopted around the policies impacting Internet of Things (IOT) technologies. Wearables, drones and autonomous vehicles are just the beginning of

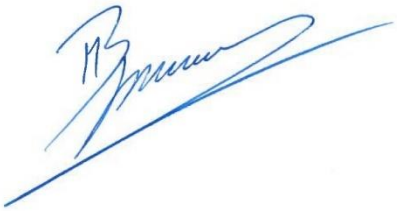
the possibilities that these relationships could forge. IoT technologies are creating new interdependencies between developers, providers and users. Furthermore, these new technologies require coordination on existing issues, such as infrastructure, skills, privacy, security and liability, in order to support global development and leadership in IOT technologies.

Ultimately, the benefits of IoT technologies will be limited only the capacity of innovators and by government decisions to allow barriers to persist rather than pursuing policies that promote innovation. To ensure IoT technologies deliver on expected benefits, the United States and the EU should avoid premature regulation that may have unintended consequences. In areas where new standards or regulation may be necessary, companies of all sizes already are leading the way. Pioneering businesses are collaborating with partners on evolving privacy and security solutions, open, consensus-driven standards, and innovative business models and use cases.

The transatlantic marketplace is a natural place for U.S. and EU firms to do business. American and EU firms support hundreds of thousands of jobs underpinned by digital trade in each other's markets. These jobs aren't just through high-tech companies: Three quarters of the value created by digital trade accrues to more traditional firms utilizing digitalization, such as manufacturers, retailers, and banks. The United States and EU have a shared interest in leading a global digital economy based on openness, innovation, and access while also safeguarding consumers, security, and democracy.

In conclusion, we look forward to working with the new teams on both sides of the Atlantic. We urge robust and continued engagement that demonstrates U.S.-EU leadership in this vitally critical area.

Sincerely,



Myron Brilliant
Executive Vice President
and Head of International Affairs
U.S. Chamber of Commerce

Markus Beyrer
Director General
BusinessEurope