NEGOTIATING OBJECTIVES FOR AN EU - US TRADE AGREEMENT

April 23, 2019

Mr Jean-Luc Demarty
Director- General for Trade, European Commission
DG Trade
Rue de la Loi 170
1049 • Bruxelles

Dear Mr Demarty,

Within the framework of the upcoming EU-US trade talks, BSA | The Software Alliance[1] would like to provide the following information regarding the priorities of the software industries for this key bilateral relation.

The EU's software industry was responsible for €1 trillion of total EU value-added growth and supported 12.7 million jobs in 2016.[2] Together, the United States and EU share an impressive $1 trillion trading relationship and make up nearly a half of global GDP.[3] This presents an enormous opportunity for the European Union and the United States to solidify a strong transatlantic partnership and build off the digital trade provisions of previous free trade agreements, such as the EU-Japan Economic Partnership Agreement and the EU- Singapore Trade agreement. This will ensure that EU innovation continues to thrive allowing for the EU digital economy to further grow.

For this reason, we have welcomed the commitment of the two blocs to start new trade talks, with the expectation that they will lead to a significant outcome on digital trade. While we were encouraged by the publication of a mandate on conformity assessment and regulatory cooperation, we strongly believe there is opportunity for these talks to consider a more ambitious agenda.

Continued EU leadership in the digital economy requires the inclusion of strong digital trade disciplines that promote the free flow of data across borders, prohibit data localization requirements, protect intellectual property, and promote interoperability, among other requirements.

The EU and the United States share common economic interests: Both enjoy a competitive advantage in the emerging technologies space, an interest in combatting digital protectionist policies abroad, and a desire to continue leading and benefiting from the digital economy. The European Union has included a

[1] BSA's members include: Adobe, Akamai, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] Software.org, The Growing €1 Trillion Economic Impact of Software (Oct. 2018), available at: https://software.org/wp-content/uploads/2018_EU_Software_Impact_Report_A4.pdf

[3] GDP (current US$), World Bank (2017): https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US-EU-1W

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

number of digital trade provisions in previous free trade agreements (FTAs) that correspond to the digital trade provisions in US FTAs. These common provisions, which would provide a sound foundation for EU-US digital trade negotiations, address:

- **The protection of source code** from mandatory disclosure requirements**;**
- **The use of electronic signatures** in commercial transactions;
- **The prohibition of preferential treatment for state-owned enterprises;**
- **The prohibition of customs duties on electronic transmissions; and**
- **Consumer choice of digital services and applications.**

We also urge DG Trade to negotiate provisions that enhance legal certainty for EU businesses in the European Union in relation to digital trade. DG Trade should work to include strong digital trade disciplines that:

- **Obligate the Parties to permit the cross-border transfer of data** while protecting personal information;
- **Prohibit data localization requirements**;
- **Promote the use of innovative technology** in the public sector;
- **Support encryption** in commercial products;
- **Protect intellectual property** while including appropriate exceptions and safeguards; and
- **Promote interoperability** through adherence to internationally-recognized standards relating to digital technologies.
- **Promote interoperable approaches to shared cybersecurity challenges**, including use of cyber security risk management frameworks

The EU has an important opportunity to set core digital standards that will not only benefit EU innovation economy but strengthen EU workforce and foster continued EU leadership in the emerging technologies and software space.

BSA's comments fall into four broad areas: securing the new data economy; updating intellectual property protections for the digital age; advancing the use of technology in government; and promoting trust and security. The driving principle in all four areas is that there should be no market access barriers and no discrimination against software.

Data Economy

Privacy and security are bedrock principles for software services providers. BSA members are committed to protecting customers' privacy and security. These companies regularly update their software products and services as well as their policies to ensure that customers are safe in using their services and other offerings, and that they comply with the laws of each market where they operate.

Ensuring that users are safe and their privacy respected are goals governments pursue as well, including through laws and regulations. Unfortunately, governments sometimes invoke these policy goals to rationalize market barriers that are intended to impede foreign companies. EU- US trade negotiations should address such barriers and ensure strong protections for digital trade.

There are several crucial commitments that EU - US negotiations should incorporate to further grow the EU digital economy and foster EU digital exports and jobs.

Free Movement of Data Across Borders: In view of the importance of cross-border data flows to the modern economy, governments should not use privacy or security as disguised market barriers or protectionist policies.

In February 2018, the European Commission released a draft text on data flows in trade agreements, seeking to address concerns from Member States, trading partners, and industry that EU FTAs suffer

from the absence of cross-border data transfer disciplines. The European Commission aims to insert the draft text into future FTAs as a way to stop third countries from restricting the flow of data through localization requirements, with the stated intention of ensuring that the EU's data protection rules are not weakened. Despite the positive intentions of the European Commission, the data flows text would actually undermine the flow of data between trading partners due to a broadly constructed exception that permits any measure a country may deem appropriate to protect personal data. This provision would permit EU trading partners to improve purely protectionist measures without any meaningful discipline.

BSA urges the EU to work with the USTR to find a more principled and effective approach to protecting cross-border data transfers while safeguarding the protection of personal information. Specifically, the EU-US agreement should obligate governments to refrain from imposing barriers to cross-border transfer of data. Recognizing that a government may determine it to be necessary to adopt or maintain measures for legitimate domestic public policy purposes, including privacy or security, that are not consistent with this obligation, such measures must not discriminate against foreign service providers or constitute a disguised restriction on trade, and must be narrowly tailored to achieve the specific objective. A dispute settlement mechanism also must be available to allow close scrutiny and enforcement of measures that derogate from this obligation.

No Localization Requirements: The agreement should preclude governments from using data localization requirements as a market access barrier in any sector of the economy. For example, a government should not require that a data center be built inside its borders as a condition for doing business in its territory.

The agreement should prohibit a government from requiring, as a condition of doing business, that a service provider use or locate computing facilities in its territory. Recognizing that a government may determine it is necessary to adopt or maintain measures for legitimate domestic public policy purposes, including privacy or security, that are not consistent with this obligation, such measures must not discriminate against foreign service providers or constitute a disguised restriction on trade, and must be narrowly tailored to achieve the specific objective. A dispute settlement mechanism also must be available to allow close scrutiny and enforcement of measures that derogate from this obligation.

Financial Services: Rules specific to any specific sector, such as financial services, which are typically addressed in separate chapters of free trade agreements, must be substantially the same as the rules of general applicability on cross border data flows and localization, and must not contain any special rules that could be interpreted to deviate from the general ones.

New Services: The agreement should ensure that robust market access commitments cover both existing services and new services that may emerge in the future. Innovative new digital services should be protected against future discrimination, and trade agreements should not become obsolete as markets evolve and technology advances.

On-line services: To promote growth of Internet-based services, the EU and US should ensure that Internet intermediaries are protected against liability for unlawful content posted or shared by third parties.

Electronic Authentication and Smart Contracts: To facilitate trade, the Agreement should require that the laws of each government allow electronic authentications and signatures to be utilized in commercial transactions. In addition, the Agreement should require governments to recognize the use of "smart" contracts and other autonomous machine-to-machine means for conducting transactions, such as blockchain, which are growing in economic significance in the EU and across the United States.

Intellectual Property

Copyright Rules: The Agreement should ensure that governments have copyright laws that provide meaningful protections for rights holders as well as safeguards to foster the Internet's continued growth as a platform for free expression, innovation, and digital commerce. The intellectual property chapter

should provide online service providers with safe harbors from liability for infringing, or otherwise unlawful, content posted by third parties. Such safe harbors require Internet service providers (ISPs) to remove infringing content upon notification by a rights holder, but should not be conditioned on any obligation by an ISP to monitor or filter infringing activity, as such obligations would weaken incentives for innovation and threaten the dynamism and values that have made the Internet so valuable.

In addition, the Agreement should preserve the ability for EU and US companies to develop world-class software-enabled data analytics solutions that are powering innovations in areas such as artificial intelligence. To that end, the Agreement should ensure that copyright laws are sufficiently flexible to permit commercial text and data mining of all lawfully accessible content.

Trade Secrets: The Agreement should require governments to adopt civil and criminal causes of action and penalties for theft of trade secrets.

Government Use of Legal Software: The Agreement should require governments to adopt laws and other measures obliging central government agencies to use only non-infringing software, and to use such software only as authorized by the relevant license for both the acquisition and management of the software for government use.

Technology in Government

Technology Promotion in Government: The Agreement should promote the use of innovative technology in government operations involving the provision of services to citizens.

Procurement: Procurement rules should be changed to reflect the 21st century needs of governments.

Choice: The Agreement should ensure that companies and government agencies are free to use the technology of their choice, and not be required to purchase and use local or other specific technology.

Trust and Security

Encryption: The Agreement should prohibit governments from undermining the use of encryption in commercial products by imposing restrictions on security technologies used to protect data in-transit or at-rest. Such a provision should preclude governments from mandating how encryption and other security technologies are designed or implemented, including imposing requirements to build in vulnerabilities or 'back doors' or otherwise requiring the disclosure of encryption keys.

International Standards: The Agreement should follow the rules agreed under the WTO Technical Barriers to Trade provisions, as updated and revised in further agreements. This is a key area for technology companies which have participated in the voluntary standards-setting processes.

Cybersecurity: The Agreement should seek to strengthen the foundations of digital trade and innovation by advancing mutually beneficial approaches to cybersecurity. The agreement should build upon previous negotiating experience, such as the principles proposed by the United Nations Group of Government Experts and endorsed by the G-7.

Cybersecurity Risk Management: Cybersecurity threats undermine digital trade in services. The Agreement should therefore encourage the mutual adoption of voluntary, standards-based, outcome-focused cyber risk management frameworks to drive the adoption of stronger cybersecurity measures by both government and industry stakeholders in key areas such as critical infrastructure and supply chains. The National Institute for Standards and Technology's Cybersecurity Framework for Critical Infrastructure, which has been strongly supported by industry at large and is currently in wide use across around the world by a variety of industries, represents one example of an outcome-focused risk management framework that has proven to be both effective and interoperable with internationally recognized standards and best practices. Each Party should promote and encourage adoption of such frameworks.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

Each party should take reasonable measures within its authority to promote alignment of Cybersecurity Frameworks within its territory and to utilize appropriate non-regulatory measures as a basis for cybersecurity risk management. The parties should also strive to eliminate any unnecessary differences in their respective regulatory measures including aligning, to the greatest degree possible, with relevant international standards, specifications, guidelines, and practices

State-owned enterprises: The Agreement should include rules precluding governments from favoring their state-owned enterprises over foreign service providers through discriminatory regulation or subsidies or via mandating the use of specific standards. The Agreement should build upon previous negotiating experience, and make these provisions enforceable through dispute settlement procedures.

No Forced Technology Transfer: The Agreement should prohibit governments from conditioning market access on the forced transfer of technology to persons in their territories. Likewise, it should preclude disclosure of trade secrets or source code as a condition of market access. These prohibitions should not, however, operate to impede legitimate security testing and research. Such provisions should be based on previous negotiating experience, and should clarify the legitimacy of security testing and research.

No Customs Duties on Electronic Transmissions: The Agreement should prohibit governments from imposing customs duties on either the telecommunications value of electronic transmissions or the value of the information being transmitted. Such a provision should be based on previous negotiating experience.

Conclusion

BSA welcomes the opportunity to provide this submission to inform the European Commission's development of specific negotiating objectives for EU-US trade negotiations. We look forward to working with DG Trade to make digital trade a central element of the negotiations. Removing market access barriers for software, and incorporating the other regulatory protections described above, will enable this growing and dynamic sector of the EU economy to expand its reach in the United States and continue to generate new jobs in the European Union.

Sincerely,

Thomas Boué
Director General, Policy – EMEA
thomasb@bsa.org
+32.2.274.1315