



## **NEGOTIATING OBJECTIVES FOR US-EUROPEAN UNION TRADE AGREEMENT**

December 10, 2018

Docket No. USTR-2018-0035

Edward Gresser  
Chief of the Trade Policy Staff Committee  
Office of the United States Trade Representative  
600 17<sup>th</sup> Street, NW  
Washington, DC 20508

Dear Mr. Gresser:

BSA | The Software Alliance<sup>1</sup> provides the following information pursuant to the request of the Trade Policy Staff Committee for written submissions regarding trade negotiations between the European Union (EU) and the United States. Our submission relates specifically to several topics on which the Committee invited comment: (1) negotiating objectives for the proposed agreement; (2) relevant barriers to trade that should be addressed in the negotiations; and (3) other measures or practices that undermine fair market opportunities.

The American software industry powers our economy – supporting over ten million American jobs.<sup>2</sup> Likewise, the EU's software industry was responsible for €1 trillion of total EU value-added growth and supported 12.7 million jobs in 2016.<sup>3</sup> Together, the United States and EU share an impressive \$1 trillion trading relationship and make up nearly a half of global GDP.<sup>4</sup> This presents an enormous opportunity for the United States and European Union to solidify a strong transatlantic partnership and build off the digital trade provisions of previous free trade agreements, such as the United States-Mexico-Canada Agreement (USMCA) and the EU-Mexico Agreement. This will ensure that US innovation continues to thrive and that our digital economy grows to reflect this.

The United States had a \$55 billion services trade surplus with the EU in 2016 – driven by US leadership in emerging technologies and innovation across the data economy.<sup>5</sup> Continued US

---

<sup>1</sup> 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.

<sup>2</sup> Software.org, The Growing \$1 Trillion Economic Impact of Software (Sept. 2017), available at: [https://software.org/wp-content/uploads/2017\\_Software\\_Economic\\_Impact\\_Report.pdf](https://software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf)

<sup>3</sup> 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](https://software.org/wp-content/uploads/2018_EU_Software_Impact_Report_A4.pdf)

<sup>4</sup> GDP (current US\$), World Bank (2017): <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US-EU-1W>

<sup>5</sup> USTR, European Union Exports, <https://ustr.gov/countries-regions/europe-middle-east/europe/european-union>

leadership in this space 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 United States and EU 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 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 US-EU 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 USTR to negotiate provisions that enhance legal certainty for US businesses in the European Union in relation to digital trade.<sup>6</sup> USTR 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.

The United States has an important opportunity to build upon the impressive digital trade achievements in the USMCA, by setting core digital standards that will not only benefit our innovation economy, but strengthen our workforce and foster continued US leadership in the emerging technologies and software space. As the White House explained, “USMCA contains the strongest measures on digital trade of any agreement. This includes rules to ensure data can be transferred cross-border and to minimize limits on where data can be stored.”<sup>7</sup> These modern digital trade provisions should therefore serve as the basis for all future agreements USTR negotiates.

Given TPA guidance<sup>8</sup> and marketplace developments, USTR accordingly has pursued updated digital trade provisions in several recent trade negotiations, including the USMCA, the Trans-Pacific

---

<sup>6</sup> See generally, <https://www.bsa.org/~media/Files/Policy/Trade/BSANTESubmission2018-10-30.pdf>; [https://www.bsa.org/~media/Files/Policy/Data/06072018LettertoEuropeanCouncil\\_CybersecurityAct.pdf](https://www.bsa.org/~media/Files/Policy/Data/06072018LettertoEuropeanCouncil_CybersecurityAct.pdf); <https://www.bsa.org/~media/Files/Policy/Data/11122018BSAfeedbackEUCompetenceCentre.pdf>; <https://www.bsa.org/~media/Files/Policy/Data/11212018BSAfeedbackEuropeanCommissionproposalpreventingterroristcontentonline.pdf>; <https://www.bsa.org/~media/Files/Policy/Data/11282018ePRNov2018jointletter.pdf>.

<sup>7</sup> President Donald J. Trump Secures A Modern, Rebalanced Trade Agreement with Canada and Mexico (2018) <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-secures-modern-rebalanced-trade-agreement-canada-mexico/>

<sup>8</sup> Congress incorporated digital trade into the principal negotiating objectives identified in the 2015 Trade Priorities and Accountability Act. Section 102(b)(6)(C) provides that agreements should “ensure that governments refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data.” Section 102(b)(6)(D) provides that “where legitimate policy objectives require domestic regulations that affect digital trade in goods and services or cross-border data flows, to obtain commitments that any such regulations are the least restrictive on trade, nondiscriminatory and transparent, and promote an open market environment.”

Partnership (TPP), the Transatlantic Trade and Investment Partnership (TTIP), and the Trade in Services Agreement (TISA). These efforts provide a foundation for modernizing US-EU trade.

BSA's comments build on the Congressionally-established negotiating objectives and recent US trade negotiations. They 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.

We urge USTR to build upon the USMCA's digital trade provisions in negotiations with the European Union. By incorporating improvements into trade negotiations with the European Union and trading partners elsewhere, the software industry can continue creating US jobs and improving the competitiveness of US industries while benefitting trans-Atlantic trade relations.

### **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 US companies. US-EU trade negotiations should address such barriers and ensure strong protections for digital trade.

There are several crucial commitments that US-EU negotiations should incorporate to grow the US digital economy and foster US 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, self-judging 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 USTR to work with the EU to find a more principled and effective approach to protecting cross-border data transfers while safeguarding the protection of personal information. Specifically, the US-EU 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. The United States must not accept broad carve-outs for future “new” services.

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

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 United States and across the EU.

## **Intellectual Property**

Copyright Rules: Consistent with US law and US free trade agreements, 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 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 21<sup>st</sup> 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 that underpin the US system.

Cybersecurity: The Agreement should seek to strengthen the foundations of digital trade and innovation by advancing mutually beneficial approaches to cybersecurity. First, 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. Second, the Agreement should encourage the mutual adoption of a voluntary, standards-based, outcome-focused cyber risk management framework to drive the adoption of stronger cybersecurity measures by both government and industry stakeholders. Such an approach should focus on the National Institute for Standards and Technology's Cybersecurity Framework for Critical Infrastructure, which has been strongly supported by US industry and is currently in wide use across around the world by a variety of US and foreign industries. The Administration's continued commitment to the NIST Framework's approach to cybersecurity is reflected in the recent executive order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

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 Administration's development of specific negotiating objectives for US-EU trade negotiations. We look forward to working with USTR and the other agencies represented on the Trade Policy Staff Committee 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 US economy to expand its reach in the European Union; contribute to an already favorable US service trade surplus; and continue to generate new jobs in the United States.