NEGOTIATING OBJECTIVES FOR A US-KENYA TRADE AGREEMENT

April 28, 2020

Docket No. USTR-2020-0011

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

Dear Mr. Gresser:

BSA | The Software Alliance[1] provides the following information pursuant to the request of the Trade Policy Staff Committee for written submissions regarding trade negotiations between the United States and the Republic of Kenya (Kenya). This 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 that should be addressed in the negotiations.

The software industry powers the American economy – supporting 14.4 million American jobs.[2] Kenya is one of several leading digitally-focused economies in an increasingly software-driven African continent. This negotiation presents an enormous opportunity for the United States and Kenya, as it creates an opportunity for both countries to establish a model for future trade agreements between the United States and other African nations, building upon the high standards of past US free trade agreements.

There are, of course, other digital trade and governance models for US trading partners to consider – models sometimes cast in terms of digital or data sovereignty that would restrict cross-border data transfers; mandate data localization; allow for an increase in digital protectionism and digital trade barriers; and permit discrimination against digital products and against new or foreign technologies, products, and services. Such digital trade policies are often grounded in assumptions that cross-border data restrictions and data localization measures will foster the creation of jobs and "local champion" enterprises, and increased domestic innovation, investment, and GDP growth. These assumptions have been widely

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] *See* Software.org – The BSA Foundation, *Growing US Jobs and GDP* (2019), avail at: https://software.org/wp-content/uploads/2019SoftwareJobs.pdf.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

refuted.[3] Development benefits from an increase – not a decrease – in connectivity and digital trade. By some estimates, just over 50% of the world's population was connected to the Internet in mid-2017, and cross-border data restrictions, localization mandates, or other restrictive digital trade policies serve to limit the economic opportunities for those who are connected.

It is essential that the United States continue to advance open, non-discriminatory, and forward-looking digital trade policies, and maintain its strong commitment to ambitious, high-standard digital trade provisions that build upon the previous US free trade agreements, such as the United States-Mexico-Canada Agreement (USMCA). Such a commitment is also consistent with the principal negotiating objectives identified in the 2015 Trade Priorities and Accountability Act, which provides that US trade 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," and which also 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."

Digital trade promotes economic development, innovation, and 21st century workforce skills. Both the United States and Kenya should capitalize on this historic opportunity to build a strong economic relationship that built on the free flow of data and other forward-looking digital policies.

As part of the agreement USTR is seeking in trade negotiations with the Kenya, BSA urges USTR to include digital trade provisions that:

- Obligate the Parties to permit the cross-border transfer of data while protecting personal information;
- Prohibit data localization requirements;
- Prohibit customs duties on electronic transmissions;
- Prohibit forced transfer of technology, including source codes and algorithms;
- Prohibit preferential treatment for state-owned enterprises; Recognize electronic signatures in commercial transactions;
- Protect intellectual property while including appropriate exceptions and safeguards;
- Support the use of innovative technology in the public sector;
- Support encryption in commercial products;
- Provide for adherence to internationally-recognized standards;
- Provide for an open regulatory environment for the trade and investment in, and development of, AI and emerging technologies, and related services; and
- Provide for non-sensitive government-generated data to be made publicly available to the public, on a non-discriminatory basis, and in machine-readable formats.

Given TPA guidance and the importance of the data economy to the future of the United States, USTR has pursued updated digital trade provisions in ongoing or recent trade negotiations including those under the auspices of the WTO Joint Statement Initiative (JSI) digital trade talks, the US-Japan Digital Trade Agreement, the USMCA, the Trans-Pacific Partnership (TPP), the Transatlantic Trade and Investment Partnership (TTIP), and the

[3] *See e.g.,* Ferracane et al., *The Costs of Data Protectionism,* VOX (2018); Ferracane et al., *Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?* ECIPE Digital Trade Estimates Working Paper No. 1 (2019); Lund et al., Defending Digital Globalization, McKinsey Global Institute (2017); Chander and Le, *Data Nationalism*, 64 Emory Law Journal 3 (2015).

Trade in Services Agreement (TISA). These efforts provide a foundation for modernizing US-Kenya trade.

BSA's comments build on these negotiations and TPA guidance. 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 and similar digital trade provisions in negotiations with Kenya. Continued US 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. By incorporating improvements into trade negotiations with Kenya and trading partners elsewhere, the software industry can continue creating US jobs and improving the competitiveness of US industries while benefitting bilateral trade relations with Kenya.

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 impede US companies.
In this regard, we outline below several crucial commitments for the US-Kenya negotiations.

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.

The 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, the Agreement should stipulate that any such measures not discriminate against foreign service providers; must not constitute a disguised restriction on trade; and must be necessary to achieve the specific objective. Furthermore, if a Party treats domestic data transfers differently from cross-border data transfers, such differential treatment must not result in less favorable treatment to a foreign service provider. Finally, 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, the Agreement should stipulate that 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 Digital Products and Services: The Agreement should ensure that robust market access commitments cover both existing categories of digital products and services and new ones that may emerge in the future. Innovative new digital products and services should be protected against future discrimination, and trade agreements should not become obsolete as markets evolve and technology advances. By design, protections for services and investment continue to apply as markets change and innovative technologies emerge, unless a specific, negotiated exception applies. 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 Kenyan governments 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.

Intellectual Property

Copyright Rules: Consistent with US law and past 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 ensure that each Party opens its government procurement market to enterprises of the other Party, including in relationship to technology, software, and cloud computing procurements.

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. 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. 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, intellectual property (IP), production processes, or other proprietary information 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.

Artificial Intelligence (AI) and other Emerging Technologies: The Agreement should provide for an open regulatory environment for the trade and investment in, and development of, AI and emerging technologies, and related services. This includes: (a) providing for ample, timely and transparent opportunities for public engagement in developing relevant policies; (b) adhering to risk-based policy development processes, including to assess and manage potential risks associated with specific AI applications; (c) taking into account voluntary, internationally recognized standards in developing technical standards and other policies; (d) giving due consideration to core principles of technological interoperability and technological neutrality; (e) ensuring that commercial data analytics in the machine learning context is permitted; (f) avoiding discrimination vis-à-vis AI applications or technologies – e.g., based on the origin of the application or technology; and (g) promoting sustained investment in AI R&D on a non-discriminatory and transparent basis.

Open Government Data: The Agreement should provide for governments make non-sensitive government-generated data freely available to the public, on a non-discriminatory basis, and in machine-readable formats.

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.

Encourage Open Digital Architectures and Ensure Technology Choice**:** Innovative companies should be able to utilize the technology that works best and suits their needs, based on open architecture and standards. The agreement should include technology choice provisions to ensure that companies are not required to purchase and utilize local technology and encourage open architecture and standards to enable greater security and drive innovation in key technologies, including cloud computing, Artificial Intelligence and 5G telecommunications.

Conclusion

BSA welcomes the opportunity to provide this submission to inform the Administration's development of specific negotiating objectives for the US-Kenya 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.