CANADA'S ACCESSION TO THE DIGITAL ECONOMY PARTNERSHIP AGREEMENT

May 3, 2021

DEPA Accession Consultations
Services Trade Policy Division (TMS)
Global Affairs Canada
111 Sussex Drive
Ottawa ON, K1A 0G2
Email: TMSconsultation@international.gc.ca

BSA | The Software Alliance[1] provides the following information in response to Canada's solicitation of comments regarding its prospective accession to the Digital Economy Partnership Agreement (DEPA).

I. Executive Summary

The software and ICT industry powers the Canadian economy – supporting nearly CA$100 billion in GDP and 700,000 Canadian jobs that pay average salaries that are 50 percent higher than the average national wage.[2] BSA members are active across the Canadian market, investing millions of dollars and employing thousands of Canadian workers every year. Participation in digital economy agreements, such as the DEPA, presents a significant opportunity for Canada's software and ICT sector. BSA strongly supports Canada's accession.

As a leading global economy, and a member of other international agreements with advanced digital trade provisions (such as the United States-Mexico-Canada Agreement (USMCA)), Canada is well positioned to propose updates to the DEPA, thus making the agreement more attractive for other countries considering accession and bolstering the agreement's status as a model for the world.

BSA proposes that the DEPA, and other digital economy agreements, should include 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;

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] *See* Industry Canada, 2019 Canadian ICT Sector Profile (2019), at: https://www.ic.gc.ca/eic/site/ict-tic.nsf/vwapj/ICT_Sector_Profile2019_eng.pdf/$file/ICT_Sector_Profile2019_eng.pdf

- Prohibit forced transfer of technology, including source codes and algorithms;
- Prohibit preferential treatment for state-owned enterprises; Recognize electronic signatures in commercial transactions;
- 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;
- Promote the responsible development of AI, including by expressly permitting data analytics in relevant laws; 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.

Beyond these core disciplines, the DEPA provides an opportunity to explore a range of new digital trade concepts, in areas ranging from digital tools and environmental sustainability, to digital inclusiveness, to digital workforce and skills development. BSA would be pleased to work with Canada to further discuss these novel concepts.

II. Discussion

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

A. Data Economy

Privacy and security are bedrock principles for software providers. Ensuring that users are safe and that their privacy is respected are goals that governments pursue as well. Nevertheless, in some cases, governments have invoked these policy goals to rationalize market barriers that impede Canadian and other North American software companies. Canada can help promote digital trade through its DEPA accession in several respects:

Cross-Border Data Transfers: In view of the importance of data transfers to the modern economy, 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; not constitute a disguised restriction on trade; and 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. DEPA's cross-border data transfer provisions could be upgraded in several of these respects. Finally, we encourage Canada to explore the openness of DEPA Parties to develop tools that will ensure that these (and other) provisions can be enforced under the agreement, such as through an effective dispute resolution mechanism.

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.

Financial Services: Rules specific to any specific sector, such as financial services, should be substantially the same as the rules of general applicability on cross-border data transfers and localization. The DEPA does not fully extend data transfer and data localization disciplines in the financial services area, in contrast to other recent agreements, including the Australia-Singapore Digital

Economy Agreement, the UK-Japan Comprehensive Economy Partnership Agreement, the United States-Mexico-Canada Agreement, and the US-Japan Digital Trade Agreement. We encourage Canada to discuss with the DEPA signatories a potential upgrade of the DEPA in this regard.

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. For its future relevance, it is important that the DEPA be designed to accommodate future developments.

On-line services: To promote growth of Internet-based services, the DEPA should explore mechanisms to ensure that Internet intermediaries receive appropriate protections from 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.

B. Digital Innovation

The DEPA should provide an enabling environment for innovation. Generalized economy-wide intellectual property disciplines need not be addressed in digital economy agreements, such as the DEPA, as these disciplines are already addressed in other agreements such as the CPTPP and the USMCA. However, there are several important innovation-related disciplines that are integral to digital technologies, which should be addressed within the agreement. These include rules on forced transfer or disclosure of source code and algorithms, rules to create an enabling environment for data analytics and AI, and rules to promote innovation in standard-setting organizations.

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 source code as a condition of market access. These prohibitions should not, however, operate to impede legitimate security testing and research.

Innovation in AI and Data Analytics: The DEPA should preserve the ability of Canadian 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 data analytics of lawfully accessible content.

International Standards: The DEPA could also provide a platform to reflect a shared commitment among the Parties to ensure application of the rules agreed under the WTO Agreement on Technical Barriers to Trade (as updated and revised in later agreements like the CPTPP and USMCA) to digital products, services, and technologies. This is critically important for innovative companies across sectors that have long participated in voluntary international standards-setting processes. Coverage should include cloud computing, cybersecurity, AI, and other emerging technologies. Reflecting a shared commitment among DEPA Parties to TBT-plus disciplines would significantly enhance legal predictability among countries that wish to improve the business and operational environment for emerging technology and innovation.

C. 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.

D. 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.

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 could also take into account the US National Institute for Standards and Technology's Cybersecurity Framework for Critical Infrastructure, which has been studied and adapted by governments around the world.

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.

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 could include: (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 copyright laws include appropriate flexibilities for commercial data analytics and machine learning processes; (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: Ensuring that quality data is available and accessible is essential for helping businesses develop and deploy innovative business practices and new products, tools, and solutions to increase their competitiveness in global markets. To unlock the value of data across their economies and to attract foreign investments, DEAs should include provisions to make non-sensitive government-generated data freely available to the public on a non-discriminatory basis and in machine-readable formats. The DEAs can also encourage the development and use of privacy-enhancing technologies that enable data collaboration in ways that align with the public's expectations for privacy.

No Customs Duties on Electronic Transmissions: The Agreement should prohibit governments from imposing customs duties or other customs requirements on software or other digital products transmitted electronically.

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. This will enable companies in participating economies to achieve greater security and drive innovation in key technologies, including cloud computing, Artificial Intelligence and 5G telecommunications.

III. Conclusion

BSA welcomes the opportunity to provide this submission to inform Canada's accession to the DEPA. We look forward to working with Global Affairs Canada on this important issue.

Sincerely yours,

Joseph Whitlock

Joseph Whitlock
Director, Policy
BSA | The Software Alliance
Email: josephw@bsa.org