08 June 2020

Australia-UK FTA Coordinator

Regional Trade Agreements Division

Department of Foreign Affairs and Trade

RG Casey Building, John McEwen Crescent

Barton ACT 0221

NEGOTIATING OBJECTIVES FOR THE AUSTRALIA-UK FREE TRADE AGREEMENT

BSA | The Software Alliance[1] provides the following information in response to the solicitation of the Australian Department of Foreign Affairs and Trade (DFAT) for comments on trade negotiations between Australia and the United Kingdom.

As Australia and the United Kingdom are recognized leaders in digital trade policy making, this negotiation presents an opportunity to establish a model for digital trade agreements around the world. It can build upon the high standards set forth in Australia's recent agreements, including the Comprehensive and Progressive Trans-Pacific Partnership Agreement, the Australia-Hong FTA, and the Australia-Singapore Digital Economy Agreement. Australia and the United Kingdom have a shared interest in advancing open, non-discriminatory, and forward-looking digital trade policies, and in maintaining their commitment to ambitious, high-standard digital trade provisions that build upon the agreements referenced above.

As part of the agreement DFAT is seeking with the United Kingdom, BSA urges DFAT to include digital trade provisions that:

- 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;

[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, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

300 Beach Road
#25-08 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

- 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.

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.

1. Securing the New 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. Unfortunately, governments sometimes invoke these policy goals to rationalize market barriers.

In this regard, we outline below several crucial commitments for the Australia-UK negotiations.

Free Movement of Data Across Borders

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 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. At the same time, 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 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.

On-line services

To promote growth of Internet-based services, the Australian and UK governments should include appropriate provisions to 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.

2. Updating Intellectual Property Protections for the Digital Age

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 Australian 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.

3. 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.

4. 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 for many years.

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.

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 Australia-UK trade negotiations. We look forward to working with DFAT to make digital trade a central element of the negotiations.

If you require any clarification or further information in respect of this submission, please contact the undersigned at brianf@bsa.org or +65 8328 0140.

Yours faithfully,

Brian Fletcher

Director, Policy – APAC

BSA | The Software Alliance