THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Digital Economy Partnership Agreement Accession Consultation

CANADIAN BAR ASSOCIATION
BUSINESS LAW, INTERNATIONAL LAW, COMMODITY TAX, CUSTOMS AND TRADE, AND INTELLECTUAL PROPERTY SECTIONS

May 7, 2021

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the Canadian Bar Association's Business Law; International Law; Commodity Tax, Customs and Trade; and Intellectual Property Sections, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Sections.

TABLE OF CONTENTS

Digital Economy Partnership Agreement
Accession Consultation

Digital Economy Partnership Agreement
Accession Consultation

I. INTRODUCTION

We are writing on behalf of the Canadian Bar Association's Business Law, International Law, Commodity Tax, Customs and Trade and Intellectual Property Sections (CBA Sections) to respond to Global Affairs Canada's consultation on Canada's interest to join the Digital Economy Partnership Agreement (DEPA).

The CBA is a national association of 36,000 members, including lawyers, notaries, academics and students across Canada, with a mandate to seek improvements in the law and the administration of justice. The Business Law Section deals with the law governing corporate entities including governance, securities regulation and commercial law. The International Law Section addresses issues of public and private international law including treaties and conventions, international trade, anti-corruption, international development and human rights. The Commodity Tax, Customs and Trade Section works on issues of commodity tax, customs and trade remedy matters. The Intellectual Property Section deals with legal issues around ownership, licensing, transfer and protection of intellectual property and related property rights.

II. GENERAL COMMENTS – BINDING OBLIGATIONS

Certain parts of the DEPA give clear requirements and obligations,[1] while other areas are largely aspirational and nebulous. The lack of binding obligations and hard targets can create inconsistencies between jurisdictions on important matters such as privacy, mutual recognition of trustmarks, interoperability and compatibility, and the potential for forum shopping.

We encourage Canada to incorporate clear obligations and measurable targets where appropriate.

---

[1] For example, Article 2.3 on Domestic Electronic Transactions Framework.

A. Module 1 (Initial Provisions and Definitions)

Article 1.1 states that the DEPA does not apply to "financial services" (except for Article 2.7 (Electronic Payments).

In our view, the DEPA should apply to financial services to empower the FinTech sector and achieve the goals of Article 8.1. The line is continuously blurring between "financial services" and other digital services – such as budgeting and personal finance software – that may require access to financial service providers' data. For FinTech businesses that rely on this data, Article 8.1's purpose will be hindered if DEPA does not apply to financial services.

We also wonder if the definition of "financial services" in Article 1.3 (cross-referencing the GATS) is consistent across jurisdictions. In the GATS, the definition of "financial services" is non-exhaustive, leaving room for interpretation. This may give rise to inconsistencies between member states.

B. Module 2 (Business and Trade Facilitation)

Article 2.3 requires Canada to "maintain a legal framework governing electronic transactions consistent with the principles of" either the *UNCITRAL Model Law on Electronic Commerce* or the *UN Convention on the Use of Electronic Communications in International Contracts*. Unless Canada's legal framework governing electronic transactions is already consistent with these UN requirements, Canada should study these agreements and consult further on the changes required should Canada join the DEPA.

Article 2.4 could add videoconferencing technology to facilitate transactions, particularly where originally signed documents may still be required (or identification verification is required). For example, consider a situation where a lawyer in one country can physically witness the execution of a document by an individual located in another country by videoconference. In 2020, videoconferencing increased significantly, and accommodations allowed originally signed documents to be witnessed on these platforms. The DEPA should recognize digital options to facilitate transactions.

Article 2.6 requires Canada to release express shipments within six hours. It is not clear if this is consistent with the Canada Border Services Agency's standard operating procedures, and whether this would result in an onerous obligation for Canada.

Article 2.6 also requires that expedited procedures apply to "shipments of any weight or value." This is inconsistent with Canada's current "Low Value Shipment" program, which allows expedited clearance for goods valued at or below a fixed amount (i.e., $3,300 CAD under the CUSMA), so the value is limited. Canada would need to consider the implications of a change to allow expedited clearance to all express shipments.

Article 2.6 would further require Canada to provide for and periodically review the *de minimis* shipment value for which customs duties will not be collected. Canada's current *de minimis* shipment value is $20 and $150 for imports from CUSMA countries. Article 2.6 does not impose an obligation on Canada to change the value but solely to periodically review it.

C. Module 3 (Treatment of Digital Products and Related issues)

Article 3.2 states that customs duties shall not be imposed on "content transmitted electronically" but allows the imposition of "internal taxes". This is consistent with Canada's commitments in other trade agreements and with the *Excise Tax Act* (and its recent amendments on the treatment of non-resident e-commerce platforms and suppliers).

With respect to cryptography, Article 3.4 should have an open-ended exemption allowing the application of local requirements to providers from member states. In other words, a member state should be allowed to require certain encryption if similar requirements apply in local law.

D. Module 4 (Data Issues)

Article 4.2(6) should consider minimum standards for the legal framework on protecting personal information. For example, Article 2.3 (Domestic Electronic Transactions Framework) requires the domestic framework to be consistent with the principles of the *UNCITRAL Model Law on E-Commerce* or the *UN Convention on the Use of Electronic Communications in International Contracts*. Similarly, Article 4.2(6) could reference international standards.[2]

Article 4.2(8) should contain minimum standards that all trustmarks must meet to qualify for mutual recognition (e.g., independent audit to confirm ongoing requirements). This will create a consistent baseline across member states for their trustmarks and enhance their reliability. A centralized portal to verify trustmarks would help ensure their credibility (e.g., Europrise Seal or the US Privacy Shield List).

---

[2] For example, the APEC Cross Border Privacy Rules, OECD Guidelines and the Convention for the Protection of Individuals with regard to Automatic of Personal Data (CETS No. 108).

In Article 4.2(10), the requirement to "endeavour to mutually recognise the other Parties data protection trustmarks" could potentially be misused or misconstrued as a barrier to trade. To avoid this risk, we suggest incorporating elements of Article 4.3(3)(a) where a measure must "not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade."

E. Module 5 (Wider Trust Environment)

We recommend defining "existing collaboration mechanism". The definition could reference the EU model in the *Directive on Network and Information Security* (NIS Directive), capturing:

- computer security incident response team (CSIRT) to promote swift and effective operational cooperation at a national and member state level and CSIRTs network (csirts-network).
- single point of contact for each member state for cybersecurity-related communications.
- members' state-level national authority for cybersecurity matters.

We are concerned with the lack of enforcement, procedure or general framework. Mutual recognition of certification schemes and minimum cybersecurity standards for digital products should also be addressed.

For Article 5.1 (Cybersecurity Coordination) we recommend establishing a central coordinating agency within the Joint Committee. We also recommend adding domestic obligations to identify each party's "national lead" on cybersecurity (like the CSIRT requirement in the EU NIS Directive) to help centralize threat reporting and coordinate on best practices.[3]

F. Module 6 (Business and Consumer Trust)

Article 6.2(10)(b) should be revised to put the focus on end-user control and decentralized data storage. This would replace an outdated consent-and-notice approach that relies heavily on a centralized holder of personal data accurately describing what it does with personal information and the individual trusting their privacy choices are respected.

---

[3] See https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2.

A focus on end-user control combined with ability to broadcast and enforce privacy choices would empower individuals. It would also catapult digital transformation and innovation by building on a growing movement of decentralization and data "sovereignty" for individuals.[4]

In Article 6.3, we recommend adding a prohibition on deceptive design or "dark patterns" like Canada is proposing in Bill C-11, *Digital Charter Implementation Act, 2020*. We believe this is especially important to ensure a clear understanding of appropriate online behaviour.

In Article 6.3, we also suggest adding a commitment to minimum online "safety" standards. There should be certain no-go zones and high standards of privacy and security, including age-appropriate design in online products and services geared toward or likely to be used by children and support for parents to make informed decisions.

G. Module 7 (Digital Identities)

Canadian businesses such as SecureKey Technologies are leaders in this area and their knowledge and expertise could be leveraged. The DEPA could also draw on emerging international use cases.[5]

H. Module 8 (Emerging Trends and Technologies)

Generally, this Module is too weak for the high-risk nature of artificial intelligence (AI) and emerging technologies. This is especially true as a global consensus is emerging on responsible AI development.[6] The non-committal language is outdated given the serious risks of developing AI or other emerging technologies with no ethical, privacy and security considerations.

---

4 Innovations include browser-based and end-user device-level preference management. The recent Apple update allowing end-users to refuse tracking by individual apps is a device-level control, as is the Do Not Track signal (though few entities recognize it and it hasn't been enforced by regulators). Tools like Privacy Cleaner by My Permissions (https://mypermissions.com/), browser-based tracking prevention using private browsers like Firefox or Brave or extensions like Ghostery, personal data accounts like Digi.Me and decentralized user ID products like Verified.Me are other examples.

5 For example, Estonia ID and its new e-Residency offering, described as a "government-issued digital identity and status that gives access to Estonia's transparent digital business environment" https://blogs.thomsonreuters.com/answerson/e-estonia-power-potential-digital-identity/ and https://e-resident.gov.ee

6 See recent activity such as the Global Privacy Assembly resolution, new European Data Protection Board draft AI regulation and Montreal Declaration. More concrete examples include the European Data Protection Board guidance on Virtual Voice Assistants, and biometrics.

In our view, Article 8.1 (Financial Technology Cooperation) is too vague. FinTech, like other innovations, can mean different things to different people. For example, FinTech includes alternative lending, consumer finance, insurtech, wealthtech, digital assets, financial services IT, payments systems, regtech, money transfer and capital markets. We wonder if FinTech referred to in Article 8.1 is meant to cover all these aspects. In addition, as discussed in our comments on Module 1, we believe the DEPA should apply to financial services to support FinTech businesses.

Article 8.2(4) states that parties shall "endeavour" to adopt internationally recognized frameworks. We recommend stronger language and incorporating examples of frameworks that the parties might consider appropriate, otherwise the requirements are too vague.

If certain member states impose rigourous standards such as algorithmic transparency, ethical AI development and bias elimination, but other members adopt a more laissez-faire approach, entrepreneurs and innovators from the "rigorous" jurisdictions be penalized as it takes longer for them to get to market than their counterparts from less regulated member states. This could lead to weakened regulation or to forum shopping. Without agreed upon high minimum standards, there is a serious risk of a race-to-the-bottom effect.

We also recommend post-market surveillance of AI-powered or emerging technology products (as is done with pharmaceuticals) to ensure products remain safe in light of new and unforeseeable risks.

With respect to government procurement, we recommend that parties incorporate the DEPA requirements in their own procurements processes. Governments are powerful purchasers and can influence the design and direction of industry. Raising mandatory minimum standards (e.g., safe, ethical and responsible AI) can have a big impact on industry.

Given the rapid pace of emerging trends and technologies, we recommend that Module 8 be reviewed every two or three years. The review may be conducted by the Joint Committee, or by another body established for the purpose of monitoring nascent technologies. Where necessary, the body should be empowered to add new technologies to Module 8.

Further, we recommend that the Parties develop a common policy for cryptocurrency payments.

I. Module 9 (Innovation and the Digital Economy)

Any data sharing projects under Article 9.4(3) should have a high level of privacy and data protection and ethical innovation built in.

Similarly, Article 9.5. should expressly reference privacy-preserving approaches to the exchanges and open data frameworks.

Intellectual Property Rights: The DEPA focuses on personal information protection and transfer of information. With respect to intellectual property (IP) rights, it would be beneficial to address issues of data innovation and licensing agreements to facilitate data sharing. Defining ownership of IP is imperative as the DEPA focuses on transmission of information across jurisdictions. Expressly defining IP ownership and rights of use would help prevent disputes and clarify the rights owners and third parties, including small and medium enterprises (SMEs).

To promote innovation and creativity, Article 9 could address the protection of online creative content (music, photos, graphics, videos, etc.) and cybersecurity to protect trade secrets (e.g., graphics, source code, object code, algorithms, programs, manuals, databases).

To support companies, especially SMEs, to use and enforce IP rights, discussions could include:

- mechanisms for content removal and protection against censorship and disinformation (e.g., spambots)
- protection, enforcement and penalties for IP infringement of data innovation, transfer and licensing
- standardizing language for online licensing, non-disclosure and encryption agreements
- education and support for SMEs on 1) how to protect their online businesses and data through IP rights and notices, insurance and licensing mechanisms; 2) public domain information, namely how to find and use material to facilitate diffusion of knowledge, technology, culture and the arts; and 3) enforcement rules of online agreements.

J. Module 10 (Small and Medium Enterprises Cooperation)

We recommend establishing a common definition or parameters and indicia of what is considered a “SME”.

DEPA member states should consider creating a jointly operated portal (a one-stop-shop) and common forms to streamline information-gathering for SMEs seeking to expand beyond

their borders. This common portal or platform would offer a single point of entry for SMEs seeking to leverage trade opportunities and obtain quick, clear information.

We suggest replacing "may" with "shall" in Article 10.3(1) to ensure each member state gives the same detailed information to facilitate market entry. It is difficult to navigate other government's information so having it all in one place would be easier.

In Article 10.4(2), digital dialogue with SMEs appears to be unidirectional. While it is important to explain the value to SMEs, this would be an excellent opportunity to hear about their pain points. It should be a two-way collaboration focusing on concrete issues that inhibit trade and market entry for SMEs. And there should be an obligation to consider and address these issues periodically.

K. Module 11 (Digital Inclusion)

Children's Privacy and Online Safety: The DEPA does not address children's privacy and online safety. We urge Canada to consider children's rights in the online environment, possibly by referencing the UN Convention on the Rights of the Child.[7] We also recommend requiring cooperation on takedown requests for non-consensual or image-based sexual abuse - like copyright infringement where takedown orders are binding.

Article 11.1(2) should add "children" as a group of requiring special attention.

We recommend that Article 11.1(3) include a mechanism for the listed groups to share their views directly with the member state, not only through their state-level representatives. Civil society groups, advocates, trade associations and not-for-profits should have an avenue for communicating directly with the parties (as intervenor, amicus or other type of status).

These groups can not be digitally included because their own governments are not inclusive. As such, relying only on governments to give them voices will perpetuate exclusion. Module 11 could also align or reference Sustainable Development Goal 8, other SDGs and Article 3 of the UN Declaration on the Rights of Indigenous Peoples (UNDRIP).[8]

---

7 See *General comment No. 25 (2021) on children's rights in relation to the digital environment*.

8 Article 3 of UNDRIP states "Indigenous peoples have the right to self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development."

Article 11(4) should be imperative rather than permissive – replace "may" with "shall". We also suggest that labour unions, civil society, academic institutions and non-governmental organisations be given an opportunity to directly engage with the DEPA's members. This could be achieved by less formal means such as online consultations.

L. Module 13 (Transparency)

The DEPA could adopt decisions by reverse consensus rather than consensus. Adopting decisions by consensus effectively gives a party a veto and can paralyze decision making, as seen in other contexts (e.g., GATT process for adopting panel reports).

M. Module 14 (Dispute Settlement)

The DEPA's dispute settlement procedures use mediation as the first form of dispute settlement, followed by arbitration. Article 14C.5 (Qualification of Arbitrators) states that all arbitrators must have expertise in "law, international trade, digital economy, other matters covered by the Agreement". This allows for arbitrators who are not lawyers or trained in the law. Canada should consider whether this should be shored up or at least clarified.

In addition, there does not appear to be a "roster" for arbitrations, unlike the CUSMA. Canada may wish to consider adding rosters of arbitrators from each of the parties to improve the DEPA.

III. CONCLUSION

We appreciate Global Affairs Canada seeking views on how the DEPA could advance international digital trade. We encourage the negotiation team to consult the CBA Sections during negotiations where necessary. We believe an opportunity to give more targeted expert input would strengthen Canada's positions.