CHAIRE DE RECHERCHE
I.A. RESPONSABLE
À L'ÉCHELLE MONDIALE

Coalition
for the Diversity of
Cultural Expressions

Study of the "Electronic Commerce" and "Intellectual Property" clauses in trade agreements

USMCA, CPTPP and DEPA Agreements

Consultation by Professor Céline Castets-Renard

Professor at the University of Ottawa, Faculty of Law – Civil Law Section
Research Chair on Accountable AI in a Global World

Reminder of the mandate

The mandate is to draft a report that may be published on the CDCE website and on the Chair's website. The report will focus on new clauses in trade agreements that may have an impact on Canada's cultural sovereignty.

The report will outline the clauses, related to electronic commerce, intellectual property rights, intermediary liability rights, and the protection of data, and explain what impacts these clauses may have.

For the CDCE, the objective is to ensure a cautious approach and an adequate representation in the face of new clauses that may limit Canada's ability to adopt or maintain measures to protect and promote its culture.

This report will cover the USMCA, CPTPP, and DEPA Agreements.

Table of Content

Summary

The **USMCA** is largely copied from American law (Section 512 DMCA Digital Millennium Copyright Act).

It imposes a system of non-liability on Internet service providers (access providers, cache service providers, hosting companies, search engines) under certain conditions. These intermediaries are not liable if they prevent access to the infringing content once they have become aware of it (notification and removal system). It establishes rules relating to notification (notice) and counter-notification to allow the defendants to express themselves (adversarial procedure). Finally, the USMCA also provides for enhanced liability when Internet service providers derive a direct financial benefit from online infringements.

To date, Canadian law provides for a system of non-liability on the sole condition that a system of notification to the copyright owner is respected (notification-notification). However, it is not clear that the adoption of the USMCA will result in major changes to Canadian law because Annex 20-B of the USMCA provides for derogations in favor of maintaining the existing law of signatory states. Therefore, less stringent rules of protection may apply and are deemed sufficient.

The CPTPP contains provisions that are adopted by the USMCA, including the "exemption regime" in the Annex.

The DEPA includes provisions related to the emergence of modern technologies such as encryption, artificial intelligence, and data governance. This new generation of agreements raises new points requiring caution.

First Agreement: Review of USMCA Agreement United States – Mexico- Canada

1. Background to the USMCA

The USMCA was concluded between the United States, Mexico, and Canada in November 2018 and entered into force on July 1, 2020. Chapter 19 deals with "digital trade." Its content is particularly broad. It also refers to Chapter 20 "intellectual property" which will be analyzed too.

2. Review of the relevant Chapter 19 (digital trade) provisions

2.1. Article 19.12: Location of Computing Facilities

Article 19.12 deals with the location of computing facilities. It provides that: "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

This provision prevents the implementation of measures relating to cloud computing facilities that store data for many digital activities of businesses and individuals. It prevents signatory states from taking measures to territorialize data storage in their territory, so that Canada could not require that data from companies doing business in Canada be located there. This provision therefore rules out the application of national sovereignty measures to the cloud and thus prevents the implementation of a "sovereign cloud."

> ***Note:*** *This measure deals with "commercial" activities and it is not clear whether cultural activities would be included and affected by this restriction. If so, this would mean that copyrighted digital content used during an activity carried on in Canada could not be mandatorily stored in Canada. In general, the fact that the computing facilities for commercial activities carried out in Canada are not located in Canada reduces the possibility of monitoring the lawfulness of those activities.*

2.2. Article 19.17: Interactive Computer Services

Article 19.17 deals with interactive computer services. Section 19.17(2) provides that: "to that end, other than as provided in paragraph 4, no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, process, transmitted, distributed or made available by the service, except to the extent the supplier or user has, in whole or in part, created or developed the information."

This provision excludes the possibility for States to establish liability rules for providers of data transmission or storage services. This measure is inspired by, but not identical to, the provisions of section 230 of the Communications Decency Act (CDA 230) and shows the

influence of U.S. law in the USMCA Agreement.[1] This measure constrains Canada's ability to make provisions to recognize the liability of technical intermediaries and should be given attention.

However, Article 19.17(4) provides exceptions to this limitation on liability in intellectual property and criminal law. Thus, the prohibition on liability measures: "(a) shall not apply to any measure of a Party pertaining to intellectual property, including measures relating to liability for infringement of intellectual property; and (b) shall not be construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right."

These rules, aimed at exempting data transmission or storage service providers from any liability, do not apply to intellectual property, which is also in line with American law and the exception provided by the DMCA (Digital Millennium Copyright Act) (Section 512) (1998).[2]

Consequently, Section 19.17(4) allows for the implementation of liability rules for data transmission or storage service providers in the case of infringement of intellectual property protected by Chapter 20, as an exception to Section 19.17(2). Chapter 20 must therefore be relied upon.

3. Review of Chapter 20 (Intellectual Property) provisions relating to internet service provider liability

Sections 20.87 and 20.88 set out liability rules that are specific to Internet service providers in relation to intellectual property. They are essentially rules of non-liability under certain

3.1 Qualification of "Internet Service Providers"

Article 20.87 first defines what is meant by "Internet service providers." Four categories of actors are concerned by this special liability regime: Internet access providers, caching service providers, hosting companies and search engines.

Internet Service Providers. Article 20.87(1)(a) states that it is: "a provider of services for the transmission, routing, or providing of connections for digital online communications without modification of their content, between or among points specified by a user, of material of the user's choosing, undertaking the function in Section 20.88.2(a)."

[1] See Vivek Krishnamurthy, Abby Lee Lenner, Meghan Sali, Velo-Vincent van Houden, Sarah Crothers, and Jessica Nguyen, Jessica Fjeld and Benjamin Horton, CDA 230 Goes *North* American?, Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States, Juil. 2020, <https://cippic.ca/en/node/129521>.

[2] Section 512 sets out exemptions to the immunity from liability for copyrighted online content provided by Section 230.

Article 20.88(2)(a) relates to: “transmitting, routing, or providing connections for material without modification of its content or the intermediate and transient storage of that material done automatically in the course of such a technical process.”

For the sake of simplicity, the section refers primarily to the Internet service providers. In addition, the internet service providers must not initiate the transmission of the content nor choose the content or its recipients. It is implied that the role of internet service providers is purely technical and that it should not intervene in the content. They must therefore remain neutral and passive.

Caching activities. Article 20.87(1)(b) then identifies the other three categories of internet service providers. These actors perform the functions in subparagraphs 2(b), 2(c), or 2(d) of articles 20.88. Article 20.88, subparagraph 2(b) addresses caching performed by means of an automated process.

This refers to "caching" activities. Technical intermediaries who perform such activities are not responsible for the temporary caching of copyrighted content for technical purposes.[3]

Hosting service providers. Furthermore, Article 20.88 2(c) refers to the storage, at the direction of a user, of material residing on a system or network controlled or operated by or for the Internet service provider. This includes storage or hosting service providers, more commonly known as content "hosts".

Hosting service providers are not responsible for the content they store for their customers, usually on servers in data centers. If they keep the data protected, the mass of stored data is such that it is impossible to foresee a systematic control of the data.

Search engines. Finally, Article 20.88(2)(d) refers to the referral or linking of users to an online location by means of information retrieval tools, including hyperlinks and directories. This includes the activities of search engines, whereby the providers of this service direct users to content that they themselves have not uploaded online.

Remarks relating to search engines. A note must be made regarding the nature of the activity of search engines, which differs from that of the other three.

The first three categories of activities are of a purely technical nature linked to the functioning of the Internet (access to the Internet, transfer, and storage of data, whether permanent or temporary (caching)). In these categories of activities, there is no interference with the data or the communication of the message. In principle, these operators have a technical, neutral, and passive role.

When it comes to the activity of search engines, however, their passivity and neutrality are questionable. Their role is more intrusive and even non-neutral by nature since search engines define keywords and settings to sort data. Search engines also refer users to

[3] In computing, a "cache" is a high-speed data storage layer that stores a subset of data, usually transient, so that future requests for that data are processed as quickly as possible by accessing the primary data storage location. Caching allows for the efficient reuse of previously retrieved or processed data. It is a purely technical operation in which the data storage is temporary.

directories or hyperlinks which involve choices that are not simply dictated by technical considerations. Therefore, search engines not purely technical, passive, and neutral by nature.

The issue here is to determine the conditions required to grant Internet service providers exemption from liability in the event of infringement on copyrighted content. It seems justified not to make them liable, if their role is indeed neutral, passive, and technical and if they do not intervene with the content. Search engines whose activity is based on algorithms for sorting and classifying content, suposing choices that may lead to the encouragement of copyright infringement, do not satisfy these conditions.

Comparison with European Union law. It is important to emphasize that Internet actors who carry out transport, caching, and hosting activities are exempt from liability under the rules applicable in European Union law, provided for in Sections 12 to 15 of Directive 2000/31/EC on electronic commerce.[4] The directive covers the first three categories outlined in the USMCA but does not provide for the inclusion of search engines, mainly because they were not considered necessary technical intermediaries required for the functioning of the Internet when the directive was adopted in 2000. Ten years later, in the Google AdWords rulings of March 2010,[5] the Court of Justice of the European Union classified them as hosting providers on the condition that their activity "is of a mere technical, automatic and passive nature."[6] Their role must then be proved on a case-by-case basis and not be pre-determined by law.

Search engines, competition law and non-neutrality. In addition, several competition laws disputes have been brought before European courts. These cases demonstrate to what extent the activities of search engines are not neutral by nature. For example, they found

[4] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32000L003>.
[5] CJUE, 23 March, 2010, Google France, Google Adwords, aff. Joined cases C-236/08 to C-238/08, ECLI:EU:C:2010:159, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=83961&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4402082>.
[6] On the basis of recital 42 of Directive 2000/31/EC.

that the search results of the Google Search engine systematically favor Google products such as Google Shopping[7] or Google Ads.[8]

Search engine business model. The business model of search engines differs from that of other internet service providers. Search engine services are offered "free of charge" and the financing of that activity is made possible by targeted advertising based on the profiling of users and the collection of their personal data. Therefore, search engines are incentivized to modify search results according to their economic interests, which confirms their ability to modify user access to content. This *modus operandi* differs fundamentally from that of other technical intermediaries (mainly hosting and Internet access providers), who charge their users for their services. Consequently, the activity of search engines is not necessarily neutral, technical, and passive and they may, in fact, pursue their own interests when deciding what content to show users in their search results.

This business model is particularly concerning as copyrighted content made freely available online becomes more popular with the public, generating higher advertising revenues for search engines and encouraging wider access to copyrighted works.

> ***Note:*** *Granting a conditional exemption from liability to Internet service providers, without requiring concrete evidence of neutral, passive, and technical behavior, is not justified in the case of search engines because the ways in which they sort and provide access to information are not neutral in themselves. Considering the business model of search engines, granting them an exception risks being harmful to the respect of protected works.*
>
> *Ideally, different conditions should be provided for search engines to be exempted from liability, either by requiring them to prove their neutrality or by excluding them from the liability exemption regime. However, section 20.88(2)(d) of the USMCA does not give states any leeway on this point. This casts doubt on the ability of the Canadian legislature to provide more stringent rules.*

3.2. Liability regime applicable to Internet service providers and remedies

[7] In June 2017, the European Commission fined Google €2.42 billion for abusing its dominant position in the search engine market by favoring its own price comparison service on Google Shopping, <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1785>.

[8] In addition, the French Competition Authority fined Google €150M for abusing its dominance in December 2019. Google abused its dominant position in the search-related advertising market by adopting opaque and difficult-to-understand rules for the operation of its Google Ads advertising platform and applying them in an unfair and random manner. As a result, the Competition Authority imposed a penalty of €150 million, and instructed Google to clarify the drafting of the Google Ads operating rules, as well as the account suspension procedure, <https://www.autoritedelaconcurrence.fr/en/press-release/autorite-de-la-concurrence-hands-down-eu150m-fine-abuse-dominant-position>.

Material scope. Article 20.87(2) states that "for the purposes of Article 20.88 (Legal Remedies and Safe Harbors), “copyright” includes related rights" i.e., neighboring rights. This is particularly important to ensure broad protection of artistic and cultural activities.

Article 20.88(2) indicates which Internet service provider activities the limitations of liability in Article 20.88(1)(b) apply to. These are the functions performed by the four categories of Internet service providers referred to in Article 20.88 i.e., the activities of "caching", hosting, Internet access and search engine (see above). These provisions therefore complement Section 20.87 and should be read together.

Subject: Remedies and Limitations of Liability. Article 20.88 deals with "Legal remedies and Safe Harbors.”[9] On the one hand, it aims to grant a right of legal recourse to copyright owners. On the other hand, it outlines the regime of conditional non-liability for "internet service providers" defined in Section 20.87.

Derogatory regime. It is further specified that Annex 20-B (Annex to Section J) applies to paragraphs 3, 4 and 6 of Article 20.88. The purpose of Annex 20-B is to nuance the implementation of the provisions of the USMCA in states party to the agreement, to facilitate the enforcement of copyright online and to avoid unwarranted disruption of markets in the online environment. The Annex then recognizes that some of the provisions in Article 20.88 do not apply to a State that is already implementing certain remedial provisions. It is therefore appropriate to also present this "derogatory" legal regime that considers the existing copyright in the States party to the USMCA, and that Canada may invoke.

1) Legal remedies for copyright owners

Legal framework for collaboration and exemption from liability. The end of Article 20.88 (1) specifies the framework governing legal remedies and exemptions from liability. On the one hand, this is based on the principle of collaboration between Internet service providers and right holders and, on the other hand, on the exemption of the latter from pecuniary liability. This provision states that: "this framework of legal remedies shall include:

a) legal incentives for Internet Service Providers to cooperate with copyright owners to deter the unauthorized storage and transmission of copyrighted materials or, in the

[9] Paragraph 1 of Section 20.88 provides the context for the protection of intellectual property rights. It states that: "Parties recognize the importance of facilitating the continued development of legitimate online services operating as intermediaries and, in a manner consistent with Section 41 of the TRIPS Agreement, providing enforcement procedures that permit effective and expeditious action by right holders against copyright infringement covered under this Chapter that occurs in the online environment." Based on the TRIPS Agreement, the section goes on to state that "each Party shall ensure that legal remedies are available for rights holders to address that copyright infringement and shall establish or maintain appropriate safe harbours in respect of online services that are Internet Service Providers.

alternative, to take other action to deter the unauthorized storage and transmission of copyrighted materials; and

b) limitations in its law that have the effect of precluding monetary relief against Internet Service Providers for copyright infringements that they do not control, initiate or direct, and that take place through systems or networks controlled or operated by them or on their behalf."

Incentives for collaboration between Internet service providers and rights holders. The legally mandated incentives are intended to prevent the unauthorized storage and transmission of copyrighted content. To this end, collaboration between Internet service providers and copyright holders is preferred. However, "other actions" are possible on a supplementary basis, which leaves room for the Canadian legislature to manoeuvre.

Diversity of collaborative efforts. Collaboration may take many forms. It may be legal or technical in nature, or a combination of both for greater efficiency. On the legal side, stakeholders may consider contractual measures that allow service providers to legally store and forward protected content. On the technical side, it may be encouraged to use work tagging devices, such as Youtube's ContentID system, which enables Youtube to identify protected content with the help of right holders.

European example. In the law of the European Union, Section 17 of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (DAMUN) institutes a combination of legal and technical measures.[10] First, point 1 recognizes that an online content-sharing service provider performs an act of communication to the public or an act of making available to the public, when it gives the public access to copyrighted works or other protected subject matter that uploaded by its users. An "act of communication to the public" or "act of making available" implies the application of copyright. The collaborative measures in Section 17 aim to structure the implementation of this copyright. Implementing such provisions presupposes a prerequisite consisting in recognizing that the activity of storing and/or transferring works without authorization constitutes an act of copyright infringement, which the European Union legislature has admitted by way of exception to the rules of exoneration from liability of technical intermediaries set forth in Sections 12 to 15 of Directive (EU) 2000/31 on electronic commerce. This directive provides a means for technical intermediaries to be exonerated from liability.

The USMCA does not recognize the liability of Internet service providers but, rather, seeks to establish the conditions required for non-liability. In European Union law, this corresponds to the E-Commerce Directive and not to the Copyright Directive. The USMCA, however, provides for a limitation of liability on the condition that Internet Service Providers do not control, cause, or command the content, even if the storage or transmission of the works would be committed by means of systems or networks that they control or operate or that are operated on their behalf. We will return to these conditions later but let us assume, as a first approach, that actors like Youtube can be considered as controlling the system. Collaborative measures would have to be implemented and it is

[10]<https://eur-lex.europa.eu/eli/dir/2019/790/oj>.

possible to draw inspiration from the collaborative measures provided for in Section 17 of the DAMUN Directive despite the differences in liability regimes explained above.

Possible collaborative legal measures: requesting permission. The primary legal collaborative measure that may be considered in the USMCA would be to obtain permission from rights holders to allow Internet Service Providers to store and make content available without infringing copyright. Several contractual forms, such as licensing agreements, can be drafted to communicate to the public or to make works or other protected objects available legally. This was how the European legislature instituted (Section 17(1) of Directive 2019/790).

Regardless of the contractual form that the Canadian legislature would like to adopt, it would be appropriate to provide that the authorizations given would also cover acts performed by the users of these Internet services when the latter are not acting in a commercial capacity or when their activity does not generate significant revenues. Otherwise, such acts could not be covered by the agreement with Internet Service Providers and would therefore require specific authorization from copyright holders. However, the threshold here should be clearly stated.

Scope of the authorization request. Logically, in the absence of authorization obtained from the rights holder, providers of content sharing services of online works should be made liable. However, the USMCA states in Article 20.88(9 that "the Parties understand that the failure of an Internet Service Provider to qualify for the limitations in paragraph 1(b) does not itself result in liability." Liability would therefore not be automatic.

For example, limitations on liability or licensing may be imposed to consider, among other things, the size and audience of the service, the cost, and resources available to the Internet Service Provider, or the novelty of the service.

Respect for copyright exceptions and limitations. Furthermore, the cooperation between Internet Service Providers and copyright holders must not lead to undermining the exceptions and limitations to copyright. Article 20.88(9) of the USMCA provides that "this article is without prejudice to the availability of other limitations and exceptions to copyright, or any other defenses under a Party's legal system."

Accountability of Internet service providers. Finally, the cooperation between Internet Service Providers and copyright holders must focus on concluding a legal agreement and ensuring its enforcement. The service providers are then the main operators of the respect or not of copyright. It would be useful to establish, for example, an obligation of information on the functioning of their practices or on the use of protected content covered by the authorization agreement. The service providers are therefore central to whether copyright is respected. It would be useful to establish, for example, an obligation to provide information on the functioning of their practices or on the use of protected content covered by the authorization agreement.

Mechanism for handling complaints, appeals and remedies. To fully satisfy Article 20.88 of the USMCA, rights holders may seek legal remedies for copyright infringement. The Canadian legislature may then decide to institute a mechanism for handling complaints and providing prompt and effective remedies in the event of a dispute over the blocking or non-blocking of access to works. Requests must be processed quickly. Furthermore, while

Internet Service Providers such as Youtube use content sorting algorithms to block protected content, automated decisions should be transparent and contestable. Ultimately, one may also decide to require that the appeal can be made to a human being who is able to render and explain the reasoning behind the final decision. Fast-track systems should not preclude alternative dispute resolution or, more importantly, judicial recourse.

> **Recommendations:** *To implement Article 20.88 of the USMCA and to comply with Section 41 of the TRIPS Agreement, the Canadian legislature must take collaborative action to enforce intellectual property rights. There are several ways in which Parliament may do this.*
>
> *First, in addition to cooperation, it could take "other actions" of its own choosing to prevent the unauthorized storage and transmission of copyrighted content. It could provide for more stringent measures against Internet Service Providers.*
>
> *Second, collaborative measures must be taken. States are free to choose whether to adopt legal or technical measures. The Canadian legislature could require a major legal measure consisting of imposing on service providers to obtain authorization from rights holders. Several contractual forms are possible, such as, but not limited to, licensing.*
>
> *If the Canadian legislature decides to institute an authorization regime for copyright owners at the expense of Internet Service Providers, it would be necessary to decide whether and under what conditions the authorization would include the acts of users of Internet services. Circumstances such as the commercial or non-commercial nature of the activity or the amount of revenue generated by the users would have to be considered and specified.*
>
> *If the Canadian legislature decides to implement an authorization regime, it should also specify whether the obligation is one of means or of result and under what circumstances the absence of a license would be acceptable. Similarly, the scope of the authorization regime could be limited according to the characteristics of the services (size, audience, financial means, novelty).*
>
> *If the Canadian legislature decides to implement an authorization regime, it should also include obligations of transparency and accountability for Internet Service Providers regarding the implementation of the collaboration, including the operation of the practices and the use of works covered by the authorization agreement.*
>
> *Article 20.88(1) of the USMCA recalls Section 41 of the TRIPS Agreement, which provides for rights holders to take effective and expeditious action against any act in the online environment that infringes copyright. Canadian legislation could provide for the implementation of a fast and effective online complaint and redress mechanism that would be available to users of services to deal with decisions to block or not block access to works. These measures should not prevent access to judicial remedies.*

2) Limiting liability of technical intermediaries

Limiting Financial Liability. Each of the Parties to the USMCA must establish or maintain appropriate liability waivers for Internet Service Providers. Article 20.88(1)(b) specifies the applicable exemption regime.

Thus, the USMCA requires each party to provide: "limitations in its law that have the effect of precluding monetary relief against Internet Service Providers for copyright infringements that they do not control, initiate or direct, and that take place through systems or networks controlled or operated by them or on their behalf."

Internet service providers are therefore exempt from monetary liability for copyright infringement committed through systems or networks that they control or operate, or that are controlled or operated on their behalf, if they "do not control, cause or command such copyright infringement."

Requirement to legally detail the financial liability limitation regime. Article 20.88(3) thus provides that "to facilitate effective action to address infringement, each Party shall prescribe in its law conditions for Internet Service Providers to qualify for the limitations described in subparagraph 1(b) or, alternatively, shall provide for circumstances under which Internet Service Providers do not qualify for the limitations described in subparagraph 1(b)."

In other words, limiting the liability of service providers implies that conditions must be met, or circumstances must be provided to exclude this limitation of liability. Article 20.88(3) contains provisions specific to hosting companies and search engines and provides additional details on the conditions to be met. The choice of these two categories of technical intermediaries is justified by their role, i.e., the fact that they intervene directly in the content.

Exemption conditions for Hosts and Search Engines: "Notice and Takedown." Article 20.88(3)(a) provides that: "These conditions shall include a requirement for Internet Service Providers to expeditiously remove or disable access to material residing on their networks or systems upon obtaining actual knowledge of the copyright infringement or becoming aware of facts or circumstances from which the infringement is apparent, such as receiving a notice of alleged infringement from the right holder, or a person authorized to act on its behalf."

This formulation corresponds to the "notice and take down" model. This model is comparable to the provisions of articles 12 to 15 of Directive 2000/31/EC, but above all to the provisions of section 512 in American law which, once again, shows its influence in the USMCA.

Limited flexibility for States. Article 20.88(3)(a) requires the Canadian legislature to change its "notice-notice" model, provided for in Article 41.26(1) of the Copyright Act,[11] and to reform its law by providing for the removal of content reported as infringing. This model of conditional liability for technical intermediaries is the middle ground between

[11] LRC 1985, ch. C-42.

complete exemption and strict liability.[12] These provisions are, a priori, an important framework for Canada's ability to develop liability rules applicable to storage and search engine activities with respect to copyrighted content.[13] However, we will see that Annex 20-B provides for exemptions allowing Canada to maintain its own regime.

There is also flexibility in the way that Internet Service Providers may become aware of copyright infringement. Notice of alleged infringement is only one example of how knowledge may be obtained. It should also be noted that the "notice of claimed infringement" comes from the right holder or a person authorized to act on his behalf. Does this mean that it cannot come from third parties or the public? Since this notice of alleged infringement is only one example of how to obtain knowledge, one can assume that States might want to expand this notice procedure.

> *Note: Section 20.88(3)(a) should compel Canada to reform its "notice-notice" system under section 41.26(1) of the Copyright Act in favour of a "notice and takedown" system modelled after the US DMCA. Schedule 20-B, however, allows states to retain provisions of their law, and the Canadian government announced in its "Consultation on a Modern Copyright Framework for Online Intermediaries" that it does not want to change its regime.*

"Good Samaritan" clause for all Internet Service Providers. Section 20.88(3)(b) provides that "an Internet service provider that removes or disables access to content in good faith under subparagraph (a) shall be exempt from any liability for having done so, provided that it takes reasonable steps in advance or promptly after to notify the person whose material is removed or disabled."

This is a "Good Samaritan" exemption from liability in the event of a removal or deactivation of content that is ultimately justified by copyright infringement. The objective is to encourage the protection of this right by not making intermediaries responsible for excessive moderation of content (over-moderation). Such a provision is favorable to the protection of copyright since the Internet Service Provider may be held liable if it does not moderate protected content "enough" but not if it moderates it "too much," which encourages action.

---

[12] S. Solomun, M. Polataiko, H. A. Hayes, "Platform Responsibility and Regulation in Canada: Considerations on Transparency, Legislative Clarity, and Design", Harvard Journal of Law & Technology, Vol. 34, Digest Spring 2021.

[13] There is no room for manoeuvre because of the mandatory language ("must"), especially since a notice of alleged infringement, as may be provided for under state law, must meet content requirements and include information that: (a) is reasonably sufficient to permit the Internet service provider to identify the allegedly infringing work, performance, or phonogram, the allegedly infringing content, and the online location of the allegedly infringing content; and (b) provides sufficient indicia of reliability with respect to the authority of the person sending the notice (footnote 122).

Notification procedures applicable to hosting providers and search engines. Article 20.88(4) requires each state to establish "appropriate procedures in its laws or regulations for effective notices of claimed infringement, and effective counter-notices by those whose material is removed or disabled through mistake or misidentification."

These provisions are intended to guarantee an easy and rapid procedure for notification of illegal content for the benefit of rights holders. They are also intended to provide a remedy for excessive takedowns and to ensure due process, as well as the right to assert non-infringement and to restore access to the content through a counter-notification. Thus, this provision also states that "if material has been removed or access has been disabled in accordance with paragraph 3, that Party shall require that the Internet Service Provider restores the material that is the subject of a counter-notice, unless the person giving the original notice seeks relief through civil judicial proceedings within a reasonable period of time as set forth in that Party's laws or regulations."

These extra-judicial measures are intended to resolve disputes quickly in the event of the removal or deactivation of content, but do not preclude legal recourse. Note that Canadian law provides for a detailed notice procedure in section 41.25(2) of the Copyright Act but no counter-notice mechanism.

Procedural measures. It is further provided that if a Party has not yet implemented the obligations set out in paragraphs 3 and 4, it shall do so in a manner that is both effective and consistent with its existing constitutional provisions. "To this end, a Party may establish an appropriate role for government that does not impair the timeliness of the process set out in paragraphs 3 and 4 or require extensive governmental review of each individual notice" (footnote 121).

The Canadian government has not yet implemented these provisions and must therefore take these sections into account when adopting accountability standards and procedures. The goal is to avoid that the copyright enforcement procedure results in the implementation of complex procedural measures that make the removal of content cumbersome and lengthy. On the contrary, Parties are invited to adopt flexible and expeditious measures, which is in line with a rapid protection of online copyrights. Nevertheless, the overriding provisions of Annex 20-B also allow the Canadian government not to comply with Article 20.88.

Sanctioning abusive infringement notifications. Another measure protects freedom of expression so that notices and infringement claims are not made improperly. Article 20.88(5) provides that "each Party shall ensure that monetary remedies are available in its legal system against a person that makes a knowing material misrepresentation in a notice or a counter-notice that causes injury to any interested party because of an Internet Service Provider relying on the misrepresentation. The term "any interested party" may be limited to copyrighted parties.

Conditions for limiting liability. Article 20.88(6) sets out the circumstances in which Internet Service Providers may avail themselves of the limited liability regime. These provisions are particularly precise and strict. Moreover, unlike all the other provisions. they are not found in the CPTTPP agreement. Two categories of requirements apply to all Internet Service Providers, while the third applies only to hosting companies and search

engines whose role is more closely related to content. They relate to the closure of repeat offender accounts and the prohibition of interference with technical measures.

Closure of recidivist accounts. Internet Service Providers are subject to a condition to be eligible for the limitations in paragraph 1: "(a) adopting and reasonably implement a policy that provides for termination in appropriate circumstances of the accounts of repeat infringers."

Operators are required to terminate service for repeat copyright infringement and to close the accounts of repeat infringers. Contrary to European Union law, this provision is not a procedure of "notification and blocking of reposting."[14] The obligation enshrined in the USMCA does not relate to the infringing content but to the accounts that post them online. This implies that a certain degree of recidivism and systematization of the infringement is required. This choice is probably easier to implement than tracing specific content, which can be particularly difficult. Canadian law does not provide for such provisions, but Annex 20-B gives States the option to waive Article 20.88 (6).

Prohibition of interference with technical measures. Article 20. 88 (6)(b) requires that Internet Service Providers: "accommodate and not interfere with standard technical measures accepted in the Party's territory that protect and identify copyrighted material, that are developed through an open, voluntary process by a broad consensus of copyright owners and service providers, that are available on reasonable and non-discriminatory terms, and that do not impose substantial costs on service providers or substantial burdens on their systems or networks."

This measure is intended to reconcile the way Internet Service Providers function with technological measures for the protection of copyrighted works. It encourages cooperation between these operators and right holders, in accordance with Article 20.88(1)(a). This substantiates the fact that incentives for cooperation may be based on legal as well as technical means. The Parties are called upon to enforce this cooperation.

> ***Note:*** *If Article 20.88(6)(b) imposes an obligation to respect technical protection measures on Internet Service Providers and is favorable to the protection of authors, its terms of application provide for reaching a consensus among stakeholders which may be difficult to achieve in practice. In addition, compliance with technical protection measures is conditioned by the obligation not to impose substantial costs or burdens on Internet Service Providers. An overly favorable assessment of these conditions could restrict the scope of protection afforded by technical protection measures, so continued attention must be devoted to the implementation of these provisions in Canada. Here again, Annex 20-B allows States to waive these provisions.*

No financial benefit for web hosts and search engines. Finally, the last provision in Section 20.88(6)(c) provides that web hosts and search engines must not "receive a financial benefit directly attributable to the infringing activity" to be exempted from liability. This seems to be a good measure, given the business model outlined above. For

[14] Article 17.4(c) of Directive (EU) 2019/790 requires technical intermediaries to provide "their best efforts to prevent them from being uploaded in the future."

instance, web hosts and search engines may have a financial interest in infringing activities because of the increased advertising revenues generated when protected works are accessed.

This raises several questions: Are advertising revenues considered a "direct" financial benefit? Is there a risk of exclusion in the presence of a sometimes complex and "indirectly" profitable business model? Furthermore, these actors must have "the right and the capacity to control such activity" that infringes copyright. Can we consider that web hosts and search engines really have a right and a capacity to control the activities they host or to which they refer? That is doubtful, and such a provision will certainly be subject to interpretation.

> ***Note:*** *The principle established in Article 20.88(6)(c), which consists of waiving the application of the liability exemption regime to web hosts and search engines that derive financial benefit from the infringing activity, is consistent with the protection of copyright. However, the conditions relating to the need for a "direct" benefit could undermine the assumption that advertising revenues are related to the content. In addition, other conditions relating to the "right" and "ability" to control the infringing activity could also exclude this condition of non-liability of these actors. Here again, Annex 20-B allows States to waive this measure.*

No general monitoring requirement. Article 20.88 (7) provides that "eligibility for the limitations identified in paragraph 1 shall not be conditioned on the Internet Service Provider monitoring its service or affirmatively seeking facts indicating infringing activity." The absence of a general monitoring requirement is due to the inability of Internet Service Providers to monitor all the content they host. Such a reservation is also allowed under U.S. law (Section 512) and under European Union law (Article 17.8 of the DAMUN Directive). However, this provision must be compatible with the technical measures specified in subparagraph 6(b).

Procedures to access the alleged infringer's information. Article 20.88(8) provides that Internet Service Providers must grant access to an alleged infringer's personal information provided that the request is made in the context of a judicial or administrative proceeding and that the request is based on "sufficient" legal grounds. It states that "each Party shall provide procedures, judicial or administrative, in accordance with its legal system, and consistent with principles of due process and privacy, that enable a copyright owner that has made a legally sufficient claim of copyright infringement to obtain expeditiously from an Internet service provider information in the provider's possession identifying the alleged infringer, in cases in which that information is sought for the purpose of protecting or enforcing that copyright."

> ***Note:*** *The Canadian Legislature should provide a rapid and easily accessible procedure. It should not require evidence of infringement that is too difficult to prove and should ensure that regulations pertaining to the protection of privacy and personal information do not prevent access to such information.*

Limits on establishing liability. Article 20.88(9) states that "the Parties understand that the failure of an Internet Service Provider to qualify for the limitations in paragraph 1(b) does not in itself result in liability." This provision may come as a surprise. Logically, it could have been understood that if the conditions for exemption from liability are not met, Internet Service Providers would have to be held liable and that this circumstance alone

would suffice. Thus, this provision reduces the protection of copyright. Furthermore, while these measures are not sufficient "on their own," reference is made to the exceptions and limitations to copyright and to the means of defense.

Enforcement of exceptions and limitations to copyright, and other means of defense. Article 20.88(9) adds that "further, this Article is without prejudice to the availability of other limitations and exceptions to copyright, or any other defenses under a Party's legal system." On the one hand, the logic of verifying the application of the conditions of the copyright system and complying with its exceptions and limitations is understandable. On the other hand, one may have reservations regarding the "other defenses," which would be given priority over copyright without further clarification being required.

If we are balancing the interests of copyright holders and the rights of the defendants in favor of those of the defendant, it is still necessary to specify which rights are at stake and how the balance between the two is struck. Otherwise, this provision amounts to a failure to give precedence to copyright as a matter of principle, which is questionable.

Implications for stakeholders. Finally, Article 20.88 (10) states that "the Parties recognize the importance, in implementing their obligations under this Article, of considering the impact on right holders and Internet Service Providers." This provides States with the flexibility to consider the impact these measures have on stakeholders.

> ***Note:*** *Caution should be exercised in the application of Article 20.88(10), which calls for consideration of the impact of Article 20.88 on stakeholders. This caveat should not lead to the consideration, for example, that the cost of enforcement would be too high for Internet Service Providers to restrict their obligations. On the other hand, it could be admissible to provide for a gradual implementation of these measures, depending on the importance of the market players. If Youtube is the dominant player and targeted specifically, it is probably not justified that the same measures apply to smaller players or to new players that may offer alternative services to the dominant Internet giants and that may play an important role in favor of the "discoverability" of more localized content. Perhaps the Canadian legislature could establish a scale of rules applicable to actors based on their traffic or market share.*

3.3. Exemption from liability based on the existing law of States (Annex 20-B - Annex to Section J)

Existing law-based exemption regime. Annex 20-B applies to paragraphs 3, 4 and 6 of Article 20.88 of the USMCA. In its first paragraph, it states that "to facilitate the enforcement of copyright online and to avoid unwarranted market disruption in the online environment, paragraphs 3, 4 and 6 of Article 20. 88 (Judicial Remedies and Liability Relief) shall not apply to a Party provided that, as from the date of agreement in principle of this Agreement, the Party continues to" provide for a number of requirements in its law.

This leaves the possibility for States to opt out of the liability regime, being the "notice and takedown" system, and to keep their law, which seems to be the will of the Canadian legislature, which wishes to preserve the "notice and notice" system.

Minimum requirements provided for by the States. Five main requirements are listed, in varying degrees of detail, to impose minimum safeguards on states party to the USMCA that must be included in their laws.

Thus, the signatory state must continue to: "(a) prescribe in its law circumstances under which Internet Service Providers do not qualify for the limitations set out in Article 20.88 (1)(b);

(b) provide statutory secondary liability for copyright infringement in cases in which a person, by means of the Internet or another digital network, provides a service primarily for the purpose of enabling acts of copyright infringement, in relation to factors set out in its law; (c) require Internet Service Providers carrying out the functions referred to in Article 20.88 (2) (a) and Article 20.88 (2) (c) to participate in a system for forwarding notices of alleged infringement, including if material is made available online, and if the Internet Service Provider fails to do so, subjecting that provider to pre-established monetary damages for that failure; (d) induce Internet Service Providers offering information location tools to remove within a specified period of time any reproductions of material that they make, and communicate to the public, as part of offering the information location tool upon receiving a notice of alleged infringement and after the original material has been removed from the electronic location set out in the notice; and (e) induce Internet Service Providers carrying out the function referred to in Article 20.88 (2) (c) (Legal Remedies and Safe Harbors) to remove or disable access to material upon becoming aware of a decision of a court of that Party to the effect that the person storing the material infringes copyright in the material."

Exceptions to the legal regime for liability. With respect to paragraph 1 (a) of Annex 20-B, it implies that even if States do not implement the legal regime of exemption from liability provided for in Article 20.88 (3), they must provide their own rules to clarify the circumstances in which the exemption from liability will not apply.

On the other hand, States must also define, in their laws, the conditions for the liability of Internet Service Providers for copyright infringement. Paragraph 1(b) of Annex 20-B provides that where a person "provides a service primarily for the purpose of enabling acts of copyright infringement," the person shall be liable.

The Canadian legislature provides for such provisions in Section 27(2.3) of the Copyright Act.

Several examples are provided by Annex-20-B, Annex to Section J, Section 1:

(i) whether the person marketed or promoted the service as one that could be used to enable acts of copyright infringement;

(ii) whether the person had knowledge that the service was used to enable a significant number of acts of copyright infringement;

(iii) whether the service has significant uses other than to enable acts of copyright infringement;

(iv) the person’s ability, as part of providing the service, to limit acts of copyright infringement, and any action taken by the person to do so;

(v) any benefits the person received as a result of enabling the acts of copyright infringement; and

(vi) the economic viability of the service if it were not used to enable acts of copyright infringement.

All of the above examples involve situations where the Internet Service Provider has encouraged copyright infringement directly and/or benefited financially from such infringement. The service is then used primarily to facilitate the performance of infringing acts. Such circumstances constitute a kind of "minimum threshold" to trigger the application of copyright and correspond to the requirements of Canadian law.

Furthermore, Annex 20-B also excludes the application of Article 20.88(6)(b) which conditions the exemption from liability of the Internet Service Provider on the fact that it does not derive a financial benefit directly from the infringing activity, in cases where it has the right and the capacity to control such activity. However, the provisions of Annex 20-B nonetheless provide for consideration of the financial interest that the service provider may have, so the exclusion is not complete and essentially reduces the level of requirement for admitting a financial benefit.

Notice of infringement regime. The exclusion in paragraph 4 has the effect of precluding the notice and counter-notice of infringement rules. Section 1(c) of Annex 20-B does, however, require that Internet Service Providers in Article 20.88 (2) (a) and (2)(c) (Internet service providers and hosting companies) participate in a system for sending notices of alleged infringement. Failing that, the service provider must be held liable for monetary damages. In other words, Annex 20-B provides States with the discretion to choose how to implement the notice but the notification itself is mandatory. Such a provision mitigates the binding nature of Article 20.88 (4), by providing States with a room for manoeuvre.

> ***Note:*** *If the Canadian legislature invokes the exemption in Annex 20-B, it must ensure that the conditions of application it establishes do not reduce the likelihood of notification of copyright infringement by the rights holder.*

Removal of content flagged by search engines. One effect of the use of Annex 20-B is to exclude Article 20.88(3), which requires service providers to remove alleged infringing content when they become aware of it, including through the rights holder's infringement notification system. However, paragraph 1(d) of Annex 20-B encourages search engines to remove content that has been flagged as allegedly infringing.

> **Note:** *The requirement standard of paragraph 1(d) of Annex 20-B is lowered by the fact that search engines are simply "encouraged" to remove content without making it mandatory. It is therefore important to be careful about the choices made by the Canadian legislature with respect to the obligation of service providers to remove content that is reported to them through tools that they have developed.*

Court decision by web hosts. In addition, paragraph 1(e) of Annex 20-B provides that web hosts are only "encouraged" to remove or disable content in the event of a court decision that the hosted content infringes copyright in that material.

> ***Note:*** *This measure is particularly weak, and a private operator must respect a decision made by a judge unless it is challenged. The choices made by the Canadian legislature must be monitored.*

Consequence: fragmented and limited protective regime. The provisions excluded by Annex 20-B relate to Articles 20.88 (3), Article 20.88(4), and Article 20.88 (6), which results in compliance with only part of this section. This leads to a fragmented legal framework which considers the existing law in each signatory state.

In addition, the provisions regarding the system of exemption from liability are finally set aside (paragraph 3) without undermining the principle (paragraph 1b). The system of notification of allegedly infringing content is also set aside, by excluding the notice and counter-notice mechanisms (paragraph 4). Finally, the measures to be taken by Internet Service Providers in the event of copyright infringement by repeat offenders, as well as the measures relating to compliance with technical protection safeguards and, to a certain extent, the provisions relating to the financial benefit derived from copyright infringement activities, are also excluded (paragraph 6).

The option for states to retain some of their existing law not only results in a fragmented law, but also reduces the standard of copyright protection and enforcement. Annex 20-B contains obligations that are less demanding than the USMCA and should be viewed as minimum requirements. In effect, states have negotiated the option not to undermine their entire law for the sake of legal certainty and reduced the standard of protection. Insofar as many USMCA provisions are inspired by American law, Mexico and Canada are the main beneficiaries of the flexibility provided by Annex 20-B. For its part, Canada has demonstrated a willingness to amend its law but without making significant changes to the liability regime.

> ***In summary: It is important to note the extent to which Canadian lawmakers will take advantage of Annex 20-B, which would reduce the standard of copyright protection provided by the USMCA.***

Second Agreement: Review of the CPTPP Agreement

(Comprehensive and Progressive Agreement for Trans-Pacific Partnership)

1. Background to the CPTPP

The free trade agreement between Canada and 10 other Asia-Pacific countries (Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam) was concluded on February 4, 2016.

2. Review of Relevant Provisions of Chapter 14 (Electronic Commerce) of the CPTPP

2.1. Article 14.4: Non-discriminatory Treatment of Digital Products

Article 14.4 (1) provides that: “No Party shall accord less favourable treatment to digital products created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of another Party, or to digital products of which the author, performer, producer, developer or owner is a person of another Party, than it accords to other like digital products.”

If this rule of non-discriminatory treatment relates to the equality of treatment of products to avoid protectionist regulations, the "digital products" in question may be works protected by copyright. It should then be emphasized that in digital matters, digital "products" are intermingled and may be of different types, leading to the application of different legal systems. In this case, the "digital products" are subject to different rules, which implies discriminating them according to their nature and not their geographical origin. Of course, this sorting does not undermine the principle of non-discriminatory treatment.

However, Article 14.4 (2) contains an exception: “Paragraph 1 shall not apply to the extent of any inconsistency with the rights and obligations in Chapter 18 (Intellectual Property).”

This provision prioritizes intellectual property rights over the principle of non-discriminatory treatment of digital products in the event of incompatibility. It is unfortunate that the primacy given to intellectual property rights only applies in cases of incompatibility and not at all times.

2.2. Article 14.13: Location of Computing Facilities

Article 14.13 (1) states that: “The Parties recognize that each Party may have its own regulatory requirements regarding the use of computer facilities, including requirements to ensure the security and confidentiality of communications.”

However, measures aimed imposing territorial requirements on digital activities are excluded at Article 14.13 (2): “No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory.”

This provision recognizes the option for signatory states to introduce measures relating to computing facilities, such as security requirements. In theory, however, states are not allowed to include provisions imposing territorial requirements on digital activities, such as the storage of data in a cloud computing system. As a result, data protected by intellectual property rights granted in Canada could be stored in a cloud outside of Canadian territory.

As an exception, however, Article 14.13 (3) provides for specific instances where the imposition of a requirement of territoriality on digital activities may be allowed: “Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.”

Provided that these obligations of non-discrimination and the principle of necessity are met, signatory states are allowed to impose territorial requirements.

In the case of cultural digital content, it is unclear whether territorial requirements may be interpreted as achieving a "legitimate public policy objective.”

2.3. Article 14.2: Scope and general provisions of the agreement

Article 14.2 clarifies the scope of the electronic commerce provisions. Article 14.2 (5) provides that: "For greater certainty, the obligations contained in Article 14.4 (Non-Discriminatory Treatment of Digital Products), Article 14.11 (Cross-Border Transfer of Information by Electronic Means), Article 14.13 (Location of Computing Facilities) and Article 14.17 (Source Code) are: (a) subject to the relevant provisions, exceptions and non-conforming measures of Chapter 9 (Investment), Chapter 10 (Cross-Border Trade in Services) and Chapter 11 (Financial Services); and (b) to be read in conjunction with any other relevant provisions in this Agreement." Article 14.2(6) adds: "The obligations contained in Article 14.4 (Non-Discriminatory Treatment of Digital Products), Article 14.11 (Cross-Border Transfer of Information by Electronic Means) and Article 14.13 (Location of Computing Facilities) shall not apply to the non-conforming aspects of measures adopted or maintained in accordance with Article 9. 12 (Non-Conforming Measures), Article 10.7 (Non-Conforming Measures) or Article 11.10 (Non-Conforming Measures)."

These Articles exempt the application of certain requirements to specific sectors, sub-sectors or activities listed in Annex II, which includes a cultural reservation:

> *"Canada reserves the right to adopt or maintain a measure that affects cultural industries and that has the objective of supporting, directly or indirectly, the creation, development or accessibility of Canadian artistic expression or content, except: (a) discriminatory requirements on service suppliers or investors to make*

> *financial contributions for Canadian content development; and (b) measures restricting the access to on-line foreign audio-visual content."*[15]

Canada rescinded both exceptions by signing letters of understanding with all the CPTPP partners following the withdrawal of the United States.[16]

In other words, the provisions relating to exceptions and non-conforming measures take precedence over Articles 14.4 (Non-discriminatory treatment of digital products) and 14.13 (Location of computing facilities). The safeguards designed to guarantee the cultural exceptions and to protect cultural industries would therefore be preserved with certain nuances.[17]

These provisions support the proper interpretation of Article 14.13 as allowing signatory states to base cultural data on their territory to achieve a "legitimate public policy objective." Articles 14.4 and 14.13 should be read in conjunction with Article 14.2 on the scope of the CPTPP Agreement to consider cultural exceptions and measures specific to cultural industries. Moreover, this combined reading suggests that provisions aimed at basing computing facilities in Canada could also apply to digital cultural content as a "legitimate public policy objective" to improve the effectiveness of intellectual property rights and cultural policy enforcement.

3. A review of Chapter 18 (Intellectual Property) Provisions for Internet Service Providers (Section J) of the CPTPP.

Purpose and Exemption (Annex 18-E). Chapter 18 of the CPTPP Agreement deals with intellectual property and includes specific provisions for Internet Service Providers (Section J). It must be noted that the framework for Internet Service Provider activities is not comprehensive and is limited to intellectual property rights. The Section J provisions apply, but the signatory parties may avail themselves of Article 17.11.23 of the United States-Chile Free Trade Agreement of June 6, 2003 (Annex 18-F). States may also avail themselves of Annex 18-E, which allows them to waive the provisions of Article 18.82 (3) and Article 18.82(4) to facilitate copyright protection on the Internet and to avoid unwarranted market disruption in the digital environment. Waiving the measures of the CPTPP provided for in the Annex is identical to the mechanism implemented in the USMCA, both in principle and in its content.

[15] Consolidated CPTPP Text - Annex II - Schedule of Canada
[16] The letters all include the same wording: "Canada may adopt or maintain discriminatory requirements on service suppliers or investors to make financial contributions for Canadian content development and may adopt or maintain measures that restrict access to on-line foreign audio-visual content.", see: Side instruments involving Canada.
[17] However, the CDCE urges some nuance on this matter. See, for example, section 4.1 of the submission on FTA negotiations with the United Kingdom and its potential participation in the CPTPP.

Definition of service providers. Section 18.81 also provides definitions comparable to those in the USMCA. It states that "Internet Service Provider means: (a) a provider of online services for the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, undertaking the function in Article 18.82.2(a) (Legal Remedies and Safe Harbors); or(b) a provider of online services undertaking the functions in Article 18.82.2(c) or Article 18.82.2(d) (Legal Remedies and Safe Harbours)." This includes transmitting, forwarding, or providing access to data (provision of network access), intermediate and transient storage (caching), storage (provision of hosting), referral or linking to an online location (search engine). These are the technical intermediary activities that are traditionally referred to in the context of digital content made available online.

Legal remedies and liability exemptions. Most of the provisions of the CPTPP are almost identical to those of the USMCA. The main difference is that Section 20.88(6) has no equivalent in the CPTPP. An important difference is the drafting of paragraph 4.

Notice of impairment and counter-notice system. Contrary to the USMCA, Section 18.82 (4) addresses the infringement notification and counter-notification system by providing for the option to institute such a system without requiring it. It provides that "if a system for counter-notices is provided under a Party's law, and if material has been removed or access has been disabled in accordance with paragraph 3, that Party shall require that the Internet Service Provider restores the material subject to a counter-notice, unless the person giving the original notice seeks judicial relief within a reasonable period of time." Since there is no such provision for deletion and reinstatement in Canadian law, this option is not significant.

Waivers in Annexes by reference to the law of the parties. Finally, the waivers provided for in Schedule 18-E have been reproduced identically in Annex 20-B of the USMCA, so reference is made to the relevant comments.

Third agreement:

A review of the DEPA (Digital Economy Partnership Agreement)

1. Background to the DEPA

The Digital Economy Partnership Agreement (DEPA) is a new type of international trade agreement launched by Chile, New Zealand and Singapore, all members of the Trans-Pacific Partnership Agreement (CPTPP). Article 1.1 provides that the DEPA only applies to measures "affecting trade in the digital economy." It entered into force on January 7, 2021, with Singapore and New Zealand completing their domestic ratification procedures. Chile is still working to complete its ratification process.

Canada is exploring potential accession to the DEPA. On December 9, 2020, Canada formally notified the parties to the DEPA of its interest in initiating discussions for possible accession to the DEPA. On February 16, 2021, Canada initiated discussions with the Parties to the DEPA. Being one of the first countries to join the DEPA would allow Canada to contribute to the evolution of the Agreement.

Why is Canada interested in joining this agreement?

The DEPA aligns with Canada's domestic and international policy objectives. These include encouraging electronic commerce as a means of facilitating international trade and enabling trade diversification for Canadian businesses, including small and medium-sized enterprises, in the near term.

The DEPA is a unique digital trade agreement in that it addresses new challenges. As digital commerce evolves rapidly, past free trade agreements have not been effective in removing or reducing the barriers faced by businesses participating in the digital economy. The DEPA is a new type of stand-alone trade agreement that focuses exclusively on facilitating digital trade.

DEPA Agreement and international initiatives at the WTO and OECD

The DEPA complements the Joint Statement on Electronic Commerce initiative currently spearheaded by the World Trade Organization (WTO). As negotiations on the WTO's Joint Statement on Electronic Commerce initiative are still ongoing, the DEPA can be viewed as an important step towards a broader multilateral agreement.

The DEPA is an autonomous and open multilateral agreement which other WTO members may join. The Agreement was constructed to be a "living agreement," allowing for continuous updating or modernization. Overall, the DEPA was designed to complement and support the ongoing WTO negotiations on electronic commerce, and to complement the work related to the digital economy underway in the Asia-Pacific Economic Cooperation (APEC), the Organization for Economic Cooperation and Development (OECD) and other international fora.

2. DEPA structure and main themes

The DEPA is divided into modules and builds on the digital trade or e-commerce chapters of existing free trade agreements, such as the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP), adding enhanced commitments to facilitate digital trade and multi-stakeholder cooperation on an array of advanced technologies.

It addresses several emerging issues related to the digital economy, including the following:

- business and trade facilitation (Module 2);
- Data issues (Module 4);
- Business and consumer trust (Module 6);
- Digital identities (Module 7);
- Artificial intelligence (module 8);
- Digital inclusion (Module 11).

In addition, the DEPA contains provisions that cover issues such as interconnection, cooperation on competition policy, the public sector, and electronic payments.

The provisions included in these modules are drawn from the CPTPP's electronic commerce chapter, and include:

- non-discriminatory treatment of digital products (Article 3.3);
- the non-application of customs duties on electronic transmissions (Article 3.2.);
- regulatory coherence (Article 1.2).

They are associated with the CPTPP chapters on:

- telecommunication services;
- cross-border trade in services; and
- technical barriers to trade;
- intellectual property; and
- financial services;
- competition policy (Article 8.4);
- small and medium-sized enterprises (Module 10);
- transparency and anti-corruption;
- dispute settlement;
- final provisions.

3. A review of the DEPA articles requiring further attention

3.1 Module 3: Treatment of Digital Products and Related Issues

Section 3.1 of the DEPA defines "digital product" as "a computer program, text, video, image, sound recording or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically." This definition is identical to that of the CPTPP and includes cultural content. Therefore, a digital product can be an item that may be protected by intellectual property and, more specifically, by copyright.

Moreover, Section 3.4 deals with information and communication technology products that use cryptography.

> ***Note:*** *Cryptography has the effect of hiding information and may be used to prevent transparency and avoid accountability. When applied to algorithms designed to sort or highlight online cultural content, these provisions may undermine any efforts to ensure transparency and accountability of the activities of online platforms such as Youtube. It may undermine any desire to implement rules of accountability towards these actors.*
>
> ***Recommendation 1:*** *Encryption measures should not be used to avoid an obligation of transparency regarding the uploading and accessing of cultural content.*

In addition, encryption measures may be implemented to protect works distributed online and guarantee the traceability of their use and prevent counterfeiting.

> ***Note:*** *The use of digital rights management (DRM) or technical protection measures (TPM), such as the ContentID system developed by Youtube, must not be prevented.*
>
> ***Recommendation 2:*** *Encryption systems must be able to be implemented to protect works and trace their use, to prevent counterfeiting (technical protection measures).*

3.2 Module 4: Data issues (personal data and computer facilities for processing and locating data for commercial use)

Article 4.2 is devoted to the protection of personal data, which is broadly defined. It provides that each party must adopt or maintain a legal framework for the protection of personal data but leaves the signatory States free to choose the kind of standards. It can be a wide or sector-based protection of privacy or personal data, or it can be a mandatory protection of voluntary measures taken by companies. The provisions also specify the principles to be adopted, as well as the requirement to provide for non-discriminatory practices with respect to the protection of personal data of electronic commerce users.

In addition, while signatory states may adopt their own regulatory requirements regarding the cross-border flow of information by electronic means, these provisions should not prevent the transfer of personal data during commercial activities.

Finally, Article 4.4 deals with the location of computing facilities, and is identical to Article 14.13 of the CPTPP. The signatory states recognize that each party may have its own regulations regarding the use of computing facilities, including requirements to ensure the security and confidentiality of communications.

However, no party shall require a person to use or locate computing facilities in their own territory as a condition for doing business in that territory. Nevertheless, this provision does not preclude a party from adopting or maintaining measures to the contrary for a public policy purpose provided that such measures do not constitute an arbitrary means, unjustifiable discrimination, or a disguised restriction on trade. In addition, this exception must not impose restrictions stricter than what is required to achieve the objective in question.

In short, signatory parties may impose security and privacy obligations on information technology infrastructure, such as cloud computing, but may not impose territorial requirements as a precondition to conduct business. By exception, territorial requirements may be imposed for legitimate public policy purposes. Thus, signatory states cannot

impose territorial requirements on computing facilities, which allows data generated by commercial activities to be located outside the territory of the state where the commercial activity is conducted.

> ***Note:*** *The data generated because of economic activity may be personal data, but it may also be* ***cultural data****. For example, if it is intended that online commercial use may include the dissemination of works. This provision is opposed to so-called "digital sovereignty"* ***location requirements****. It may constitute a weak point in the protection of protected works in Canada since their processing and storage may take place outside Canadian territory. The loss of physical control over the data makes it more difficult to ensure compliance with Canadian copyright law.*
>
> *This clause requires caution because it could limit Canada's ability to adopt or maintain measures that protect copyright. Unless, of course, if copyright protection can be considered a "legitimate public policy objective" and be subject to the exception, which requires further clarification.*
>
> *Nevertheless, this caution may be lifted or at least mitigated by reviewing Annex 1, which states that certain articles of the DEPA (referring to Article 4.4 specifically) do not create any rights or obligations between or among the parties.*

3.3 Module 8: Artificial Intelligence (AI)

Article 8.2 of the DEPA includes provisions on intellectual property, stating that the parties shall endeavor to promote the adoption of ethical and governance frameworks that support the trusted, safe, and responsible use of AI technologies. Specifically, the parties shall endeavor to take into consideration internationally recognized principles or guidelines, including values of “explainability”, transparency, fairness, and human-centred values.

> ***Note:*** *While adopting ethical values and Artificial intelligence governance frameworks should be encouraged, these measures must not detract from the law and the obligation to respect the rules of law. In particular, artificial intelligence relies on the use of massive amounts of data, some of which may be protected by intellectual property rights.*
>
> ***Recommendation 3:*** *Before any new ethical considerations, it is necessary to recall the obligation of complying with the rule of law and with intellectual property rights in the deployment of an artificial intelligence system.*

This also raises the question of respecting copyright when creating works using machine learning processes that are based on pre-existing works.

> ***Note:*** *The question is whether to support an exception for the use of copyrighted works, when such works constitute big data, are used in the creation process by artificial intelligence (machine learning, for example), and give rise to the creation of new works whose authorship may be disputed. Existing* exceptions *such as fair use or non-commercial user-generated content could not be invoked.*
>
> ***Recommendation 4:*** *It must be recalled that copyright does not provide a specific exception for when big data includes protected works and is used to create new works generated by artificial intelligence, and this constitutes an infringement of copyright.*

3.4. Module 9: Innovation and the digital economy

Module 9 is about open data and data innovation. Article 9.1 defines open data as "digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed. This definition relates only to information held or processed by or on behalf of a Party."

Article 9.4 goes on to address data innovation. "The Parties also recognise that data sharing mechanisms, such as trusted data sharing frameworks and open licensing agreements, facilitate data sharing and promote its use in the digital environment to: (a) promote innovation and creativity; (b) facilitate the diffusion of information, knowledge, technology, culture and the arts; and(c) foster competition and open and efficient markets."

> ***Note:*** *This probably relates to data trusts with cultural purposes. Data trusts are founded on the trust of sharing protected information on the condition that clear rules are established, with specific emphasis on the standards imposed on the trustee. Nevertheless, various models and mechanisms of data trusts can be conceived, depending on the cases considered and the legal systems involved. Even within Canada, the common law data trust is not identical to the Quebec Civil Code data trust. Consequently, even if cultural data is the focus, the rules proposed here are too vague to ensure the proper safeguarding of protected data, and to guarantee that the protected data is used in a manner that is consistent with the objectives of the trust.*
>
> ***Recommendation 5:*** *The rules governing data trusts for cultural purposes must be clarified, especially regarding the purposes for which they are to be used and the guarantees provided to ensure compliance.*

In addition, Article 9.5 encourages the opening of government data.

> ***Note:*** *Here too, we must be careful with the opening of government data because the data stored by government agencies may include data belonging to third parties that are protected by intellectual property rights. Therefore, the opening of government data requires a case-by-case assessment of the data concerned and a search for any rights that might be attached to it. In addition, it is also recommended to introduce public licenses on this data and make it available online. Such licenses should not automatically confer rights to content that is protected by intellectual property.*
>
> ***Recommendation 6:*** *Clarification is needed regarding the exclusion of the intellectual property rights of third parties when opening government data.*

3.5. Module 15: Cultural Exceptions

The cultural exception provided for in Article 15.1 (4) differs significantly from the clauses traditionally negotiated and concluded by Canada. This should not be surprising given that DEPA was not negotiated with Canada.

> ***Note:*** *The notion of "creative arts" is central to the provision. It includes activities beyond cultural industries which are traditionally creative oriented industries. The creative arts listed here are either new (digital) or have long been ignored*

(Aboriginal art). Therefore, one interpretation may be that: 1) this clause does not challenge the classical conception of cultural exception clauses usually upheld by Canada, notably as provided for in the CPTPP; 2) this clause is complementary in that it may be interpreted as going beyond the traditional cultural exception clauses. The reference to "creative arts" would therefore be complementary and go further than the traditional cultural industries. It must also be noted that DEPA complements the CPTPP agreement to which the three DEPA signatory states are parties. This reinforces the idea of the complementarity of rules. In addition, DEPA emphasises, at various points in the text, the importance of remaining consistent with their existing laws. Thus, Article 1.2. states that the intention of the parties is for this agreement (DEPA) to co-exist with their existing international agreements (for example, CPTPP).

Recommendation 7: *The content of the cultural exception provision must be clarified and must include the principles of protection of cultural industries that Canada has traditionally defended.*