ARTICLES

EXPORTING THE FIRST AMENDMENT THROUGH TRADE: THE GLOBAL "CONSTITUTIONAL MOMENT" FOR ONLINE PLATFORM LIABILITY

HAN-WEI LIU*

ABSTRACT

The United States in the recent United States-Mexico-Canada Agreement and Japan-U.S. Digital Trade Agreement adopts a new clause which mirrors Section 230 of the Communications Decency Act of 1996, shielding online intermediaries from third-party contents liability. For policymakers, the seemingly innocuous "Interactive Computer Services" title creates the fundamental challenge in balancing free speech against competing interests in the digital age. This Article argues against globally normalizing this clause through its diffusion in trade deals. Internally, as the Biden Administration has offered a clean slate to discuss reforms to the controversial regime, it is unwise for U.S. trade negotiators to export the same clause in future negotiations. Externally, it is problematic for other partners to accept this clause, born from American values deeply rooted in the First Amendment. Each country is entitled to achieve the fundamental right of free speech through their own economic, social, and political pathways, towards an optimal balance—and rebalance—against other interests. The clause should be dropped from future trade negotiations while policymakers worldwide grapple with the challenges posed by online platforms and reconfigure their regulatory frameworks in the digital era.

---

* Senior Lecturer, Monash University, Australia. Earlier drafts of this paper were presented at the 2021 Biennial Conference of the Asian Society of International Law, the European Society of International Law (ESIL)-Kraków-Leiden Second Symposium on "Exploring the Frontiers of International Law in Cyberspace," the Seventh Biennial Global Conference of the Society of International Economic Law (SIEL), and the 2021 Online Research Workshop on Digital Trade Law Governance in the Asia-Pacific by National Yang Ming Chiao Tung University School of Law (Taiwan). The author is grateful for the comments of the participants of these conferences and would like to thank Petros Mavroidis (Columbia), Ching-Fu Lin (National Tsing Hua University), Thomas Streinz (NYU), Mengyi Wang (Graduate Institute, Geneva), and Lucia Oriana (UNSW) for their comments. The author thanks Tiana Moutafis, Grace Pittar, Lourdes Luna Valdez, Guanqing Liu, and Max Davie for excellent research assistance. The author can be reached at han-wei.liu@graduateinstitute.ch.

I. INTERACTIVE COMPUTER SERVICES: WHAT IS IN THE NAME?

International trade agreements have been viewed by some—especially major trading powers like the United States (U.S.)—as a promising tool to export their domestic laws, substantive or procedural, in the name of harmonization. On substantive laws, a prime example is that the U.S. has pursued intellectual property rights (IPRs) through preferential trade agreements (PTAs).[1] Likewise, the U.S. has attempted to

1. *See, e.g.*, Kenneth Chiu, *Harmonizing Intellectual Property Law Between the United States and Singapore: The United States—Singapore Free Trade Agreement's Impact on Singapore's Intellectual Property Law*, 18 GLOB. BUS. & DEV. LAW J. 489, 499 (2005) (reporting that in the early 2000s, Singapore did not "appear to have an interest in increasing intellectual property" for the lack of "a large amount of intellectual property owners within its borders" and although it is true that Singapore viewed "adopting foreign standards as a part of trade agreements" to strategically benefit its economic development, it is also obvious that the U.S. has leveraged the trade negotiations by requesting Singapore to align its IPRs laws with those of its own). On this score, see generally Margot E. Kaminski, *The Capture of International Intellectual Property Law Through the U.S. Trade Regime*, 87 S. CAL. L. REV. 977, 983–89 (2014) (outlining the sea change of the U.S. trade policy in relation to IPR protection and suggesting that the IPR arrangements in the U.S. trade agreements

export its Administrative Procedure Act (APA) type of rulemaking process by the "regulatory coherence" or "good regulatory practices" mechanisms in recent mega-regional pacts, notably, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States-Mexico-Canada Agreement (USMCA).[2] With the data-driven economy continuing to grow and "Big Tech" penetrating virtually every corner of our digital life,[3] the U.S. has quietly set yet another foothold for its high-tech firms by exporting Section 230 of the Communications Decency Act of 1996 (CDA 230) in the name of "Interactive Computer Services" under the USMCA and later the Japan-U.S. Digital Trade Agreement (Japan-U.S. DTA).[4]

While aligning the normative order of the online environment with U.S. domestic laws and policies through international trade and investment agreements is nothing new,[5] much of the existing literature focuses more on American efforts pushing the unfettered cross-border data flow and the implications of the U.S.-EU divide on data protection

---

are "close to, but not precisely, the U.S. law"). One may however argue that such a pattern predated the turn to free trade agreements and thus influenced the Uruguay Round and the TRIPs Agreement.

2. Comprehensive and Progressive Agreement for Trans-Pacific Partnership ch. 25, *opened for signature* Mar. 8, 2018, [2018] A.T.S. 23. (entered into force Dec. 30, 2018) [hereinafter *CPTPP*] (incorporating, by reference, the provisions from the Trans-Pacific Partnership). Although the U.S. has left the TPP, Chapter 25 on Regulatory Coherence remains intact. See Agreement between the United States of America, the United Mexican States, and Canada ch. 28, Nov. 30, 2018, Office U.S. Trade Rep., https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between [hereinafter *USMCA*]. For a detailed analysis of the global norm diffusion of regulatory coherence, see generally *Regulatory Rationalisation Clauses in FTAS: A Complete Survey of the US, EU and China*, 19 MELB. J. INT'L L. 1 (2018).

3. The term "Big Tech" often refers to four major technology firms in the U.S., including Facebook, Apple, Google, and Amazon (FAGA). Occasionally, Microsoft is added to the list. *See, e.g.*, Richard Waters, *Move Over Faangs, Make Way for Maga*, FIN. TIMES (July 28, 2018) (referring to "Maga" as including Microsoft, Apple, Google, and Amazon).

4. CDA 230 is, in short, the provision that affords online intermediaries broad immunity in respect of legal claims arising from the content posted by users on their platforms. Communications Decency Act of 1996, Pub. L. No. 104-104, §502, §223 (a), (e)(5), 110 Stat. 56, 133-34 (1996) (codified as amended at 47 U.S.C.A. § 230 (2018)); see Agreement between the United States and Japan Concerning Digital Trade, Japan-U.S., Oct. 7, 2019, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf [hereinafter *Japan-U.S. DTA*].

5. Some commentators however argue that the U.S. trade policy has not adequately addressed the digital economy and its contributions. *See, e.g.*, Markham C. Erikson & Sarah K. Leggin, *Exporting Internet Law Through International Trade Agreements: Recalibrating U.S. Trade Policy in the Digital Age*, 24 CATH. U. J. L. & TECH. 317, 318 (2016).

for global trade.[6] Thus far, this new provision has received scant scholarly attention with a set of analytical questions left unresolved: What falls within "Interactive Computer Services"? Why did the U.S. include this new clause in the USMCA and Japan-U.S. DTA? What are their normative implications for its trading partners? How likely would such a new clause emerge as a new template to be included in other PTAs going forward?

By addressing these questions, this Article makes three major claims. First, behind the seemingly innocuous "Interactive Computer Services" title lies a fundamental challenge facing policymakers in the digital era—whether and to what extent online platform companies should be liable for content made available by its users, such as hate speech or defamatory statements. For the first time in its trade agreements, the U.S. requires its trading partners to adopt what I coin an "*Intermediary Immunity*" clause. Such a clause mirrors CDA 230 to immunize providers and users of "interactive computer services" regarding third-party content and the removal of content under some circumstances.[7] This clause appears purely economic-oriented by claiming to promote interactive computer services "vital to the growth of digital trade."[8] However, this innocuous formulation obfuscates a central concern: the freedom of expression in the digital era. The complexity of the underlying interests around regulating online speech might explain why the U.S. has sought to downplay this new regulatory mechanism by using the rather modest name, "Interactive Computer Services." This is in sharp contrast to what we have seen in a related context: the U.S. was not shy in calling the rules concerning online intermediaries' liabilities for copyright infringement "Legal Remedies and Safe Harbors" when

6. A handful of exceptions written by trade lawyers, *see* Joshua P. Meltzer, *The United-Mexico-Canada Agreement: Developing Trade Policy for Digital Trade*, 11 (2) TRADE, L., & DEV. 239, 255 (2019). Most commentaries come from law and tech scholars. *See* Vivek Krishnamurthy & Jessica Fjeld, *CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States*, https://techlaw.uottawa.ca/news/cippic-releases-new-report-intermediary-liability-canada-and-united-states (last visited Jan. 4, 2020) [hereinafter Krishnamurthy & Fjeld, *CDA 230 Goes North American*]; see Michael Geist, *From Copyright Term to Super Bowl Commercials: Breaking Down the Digital NAFTA Deal*, https://www.michaelgeist.ca/2018/10/from-copyright-term-to-super-bowl-commercials-breaking-down-the-digital-nafta-deal/ (last visited Jan. 20, 2021) [hereinafter, Geist, *From Copyright Term to Super Bowl Commercials*]; see Angelina Fisher & Thomas Streinz, *Confronting Data Equality* 53-54 (IILJ Working Paper 2021/1), https://www.iilj.org/wp-content/uploads/2021/04/Fisher-Streinz-Confronting-Data-Inequality-IILJ-Working-Paper-2021_1.pdf (focusing on this CDA 230-like provision's implications for global data inequality).

7. 47 U.S.C.A. § 230 (2018).

8. USMCA, *supra* note 2, art. 19.17.1.

exporting the Digital Millennium Copyright Act (DMCA) through trade agreements years ago.[9]

Second, the primary motivation of baking the CDA 230-type clause into trade deals is to lock the U.S. into the existing regulatory framework. On a surface level, the Intermediary Immunity clause could help entrench American online platform firms like Facebook and Twitter into the global online environment by minimizing their legal risks of doing business abroad.[10] Upon deeper analysis, however, the effect of this new provision is not as sweeping as it appears to be—at least not in the case of Japan and Mexico. Japan and Mexico have both minimized the effect of this CDA 230-like arrangement through the Side Letter or the Annex, in contrast with Canada welcomed it without qualification to create a level playing field in attracting online businesses.[11] The fact that the U.S. did not take a hardline approach towards Japan and Mexico by allowing various carve-outs can only cast doubt on how seriously the U.S. seeks to export its CDA 230 to its trading partners.[12] CDA 230 has long received enormous criticisms at home. CDA 230 has been

9. *See, e.g.*, Australia-U.S. Free Trade Agreement, Austl.-U.S., art 17.11.29, signed May 18 2004, [2005] A.T.S 1 (entered into force Jan. 1, 2005)*; see* United States-Singapore Free Trade Agreement, Sing.-U.S., art. 16.9.22, signed May 6, 2003, [2004] (entered into force Jan. 1, 2004); *see* United States-Chile Free Trade Agreement, Chile -U.S., art. 17.11.23 [2004] (entered into force Jan. 1, 2004); see *United States-Colombia Trade Promotion Agreement,* Colom.-U.S., art. 16.11.29, signed Nov. 22, 2006, [2012] (entered into force May 15, 2012); see *United States-Bahrain Free Trade Agreement,* U.S.-Bahr., art. 14.10.29, signed on Sept. 4, 2004, [2006] (entered into force Jan. 11, 2006); see United States-Morocco Free Trade Agreement [2004] (entered into force Jan. 1, 2006) art. 15.11.28; see United States-Dominican Republic-Central America Free Trade Agreement [2005] (entered into force Mar. 1, 2006 in El Salvador, Apr. 1, 2006 in Honduras and Nicaragua, July 1, 2006 in Guatemala, Mar. 1, 2007 in the Dominican Republic, and Jan. 1, 2009 in Costa Rica) art. 15.11.27; see United States-Peru Trade Promotion Agreement [2006] (entered into force Feb. 1, 2009) art. 16.11.29; see United States-Panama Trade Promotion Agreement [2007] (entered into force Oct. 31, 2012) art. 15.11.27. There are two possible explanations of calling this safe harbor clause as the "Interactive Computer Services." One, a more conspiracy theory, is that the US attempted to "hide" this controversial clause, given the increasing significance of regulating online platforms' liabilities in the US and elsewhere. However, such a conspiracy theory may be reading into the text, as DCMA and other arrangements could be equally, if not more, controversial, when they were included in trade deals. Therefore, an alternative yet innocent explanation might well be that the US trade negotiators simply drew the relevant terminologies from CDA 230, as a technical matter. The author is grateful to Thomas Streinz for pointing this out.

10. *See, e.g.*, *The USMCA impacts the Canadian Intermediary Liability Regime, Digital Watch* (Nov. 16, 2018), https://dig.watch/updates/usmca-impacts-canadian-intermediary-liability-regime/ (observing that this provision may, depending on how it is implemented in Canada, affect the Canadian system of intermediary liabilities).

11. *See* discussion *infra* Part II.C.3.

12. *See infra Part II.C.3.*

a major battlefield, politically and legally, in the U.S. over the past few years—and the 2020 Presidential election elevated the relevant debates to a new level. During the USMCA negotiations, congresspersons voiced their concerns that it should have been reformed at home first before exporting such a controversial clause.[13] The exportation of CDA 230 through trade, while generously accommodating for various qualifications, seems to suggest that the primary motivation of including the Intermediary Immunity clause is to help lock the nation within the existing framework, making it more difficult for lawmakers to overhaul CDA 230 at home.[14]

Third, it seems undesirable and impracticable to further diffuse the Intermediary Immunity clause as a new global norm through trade negotiations. While the U.S. has incorporated this clause in the USMCA and Japan-U.S. DTA, and recently proposed similar language in the consolidated negotiating text for the WTO Electronic Commerce Negotiations,[15] those dynamics concerning how online platforms should be regulated in the U.S. and beyond would constitute *internal* and *external barriers* for the CDA 230-type arrangement to be included in future PTAs. Internally, President Biden has offered a clean slate for both Republicans and Democrats and the White House to discuss reforms anew.[16] Presumably, it is unwise for the U.S. trade negotiators to export the same clause in future negotiations if the Biden Administration is serious about reconfiguring the old regime. Externally, it is problematic for other trading partners to accept this new clause—one that features American values deeply rooted in the First Amendment. While it is true that free speech is a fundamental human right, it is equally true that each country has, and is entitled to, their own pathways to achieve it. Different pathways reflect the divergent economic, social, and political factors in progressing towards an optimal balance—and rebalance between free speech and other competing values. The Intermediary Immunity clause should be dropped out from future trade negotiations, while policymakers worldwide are

13. Lauren Feiner, *Pelosi pushes to keep tech's legal shield out of trade agreement with Mexico and Canada, CNBC,* https://www.cnbc.com/2019/12/05/pelosi-pushes-to-keep-section-230-out-of-usmca-trade-agreement.html (Dec. 5, 2019, 12:16 PM). *See infra* note 188 and accompanying text (describing the concerns raised by Frank Pallone, Jr., and Greg Walden in relation to the CDA 230-like language in USMCA).

14. Of course, it is not clear whether the US lawmakers would consider this international commitment if they are serious about the CDA 230 reform at home.

15. Consolidated Negotiating Text, WTO Electronic Commerce Negotiations, WTO Doc. INF/ECOM/62/Rev.1 (Dec. 2020) [hereinafter *WTO 2020 E-Commerce Negotiation Text*].

16. *See infra* note 209 and its accompanying text.

grappling with the critical challenges posed by online platforms and reconfiguring their regulatory frameworks in the digital era.

Against this backdrop, the remainder of this Article proceeds as follows. Section II offers a critical assessment of the normative implications of the Intermediary Immunity clause from the perspective of international trade law. The legislative history and jurisprudence around CDA 230 are crucial to our understanding of this new clause under USMCA and Japan-U.S. DTA. Although it is true that CDA 230 and the Intermediary Immunity clause are subject to different principles of interpretation, the root, structure, and application of CDA 230, as read and applied by the U.S. courts as per legislative intent, can be informative on at least two fronts. First, an understanding of the operation of CDA 230 helps shed light on how industry stakeholders may act and build upon their expectations of the new clause under the USMCA, Japan-U.S. DTA, and beyond. This is especially true, given that the Intermediary Immunity clause is a novel one, only having been introduced to the PTA recently. CDA 230 experience would presumably serve as a critical anchor for high-tech firms —and the trade policymakers acting on their behalf in shaping their strategic decisions.

Second, and more crucially, the background of CDA 230 can illuminate what the "Interactive Computer Services" clause means and what interests are at stake, thereby indicating how far this new mechanism could go in the future. Part III makes the case against the normative diffusion of CDA 230 through trade deals by identifying the internal and external limitations. It first reflects on the underlying rationale of introducing the Intermediary Immunity clause through trade negotiations by placing it within the U.S. domestic politics surrounding CDA 230. These dynamics not only help make sense of why the U.S. does not take a hardline approach towards this new clause but also constitute the internal limitations of CDA 230 to be further diffused through trade agreements. Equally important is the external boundary. By exploring the compatibility of the Intermediary Immunity clause with the existing laws of other trading powers, notably, E.U. and China, this Article illustrates how different regulatory models governing online platforms may work as hurdles for CDA 230 to emerge as a new global norm through international trade negotiations. Part IV concludes the discussion of CDA 230 and Intermediary Immunity.

II. Shaping the Normative Order of Online Speech Through Trade

A. *The Rise of the Intermediary Immunity Clause in Trade Agreements*

The USMCA, a successor to the North American Free Trade Agreement (NAFTA), took effect on July 1, 2020.[17] Like many PTAs,[18] the USMCA has a dedicated chapter on e-commerce—albeit a different title called "Digital Trade."[19] Unlike others, however, the USMCA goes beyond topical issues like data localization,[20] personal information protection,[21] having domestic laws and regulations in line with the UNCITRAL Model Law on Electronic Commerce 1996,[22] paperless trading,[23]and source code by adding an innovative mechanism—the Intermediary Immunity clause in Article 19.17.[24] With recognizing "the importance of the promotion of interactive computer service, including for small and medium-sized enterprises, as vital to the growth of digital trade,"[25] Article 19.17.2 of USMCA provides that:

17. *See* Press Release, Office of the U.S. Trade Rep., United States-Mexico-Canada Trade Fact Sheet: Modernizing NAFTA into a 21st Century Trade Agreement (Oct. 2018), at https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing.

18. The PTA between Australia and Singapore in 2003 is the first one with a dedicated chapter on e-commerce. Moreover, as per Mira Burri, of 348 PTAs entered into between 2000 and 2020, there are 185 containing provisions relating to digital trade; 80 have a standalone e-commerce chapter. See Mira Burri, *Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions*, paper presented at the Singapore Management University School of Law Conference on the Roadmap to the ASEAN-EU FTA in the Post-Pandemic Era (Dec. 3, 2020) (on file with the authors) [hereinafter Burri, *Approaches to Digital Trade*]; see Mark Wu, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, ICTSD (2017), http://e15initiative.org/publications/digital-trade-related-provisions-in-regional-trade-agreements-existing-models-and-lessons-for-the-multilateral-trade-system/.

19. USMCA, *supra* note 2, ch. 19.

20. *See, e.g.*, CPTPP, *supra* note 2, art. 14.13. Note, however, that the USMCA has, unlike the CPTPP, imposed the prohibition on data localization in the context of financial services, subject to certain exceptions. *See* USMCA, *supra* note 2, art. 17.17.

21. *See, e.g.*, CPTPP, *supra* note 2, art. 14.8.

22. *See, e.g.*, *id.* art. 14.5.

23. *See, e.g.*, *id.* art. 14.9.

24. *See, e.g.*, *id.* art. 14.17; USMCA, *supra* note 2, art. 19.17.

25. CPTPP, *supra* note 2, art. 19.17.1. To be sure, including such an immunity can help SMEs reduce their operational costs. As Eric Goldman aptly pointed out, "new marketplace entrants do not need to make the upfront investments into content moderation that Google and Facebook make. If new entrants had to develop industrial-grade content moderation procedures from day one, we would see far fewer new entrants." See Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, *in* Oxford Handbook of Online Intermediary Liability 157, 163 (Giancarlo Frosio ed., 2020) [hereinafter Goldman, *An Overview of Section 230*].

> . . . 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, processed, 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.[26]

The term "interactive computer service" is defined under Article 19.1 as "a system or service that provides or enables electronic access by multiple users to a computer server,"[27] a term that is broadly defined and has attracted disputes in the U.S. law context, as elaborated below. Article 19.17.3 further extends the immunity for interactive computer service providers' actions to edit harmful or objectionable materials and actions that enable content providers to restrict access.[28] It provides that:

> No Party shall impose liability on a supplier or user of an interactive computer service on account of: (a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable; or (b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable.[29]

The Intermediary Immunity clause, however, creates some carveouts. Article 19.17.4 clarifies its scope of application that this immunity clause shall not apply to "any measure . . . pertaining to intellectual property, including measures addressing liability for intellectual property infringement" nor shall it be "construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right."[30] It also makes clear that the Intermediary Immunity clause shall not be read to prevent "a Party from enforcing any criminal law," or "a

26. CPTPP, *supra* note 2, art. 19.17.2.

27. *Id.* art. 19.1.

28. CPTPP, supra note 2, art. 19.17.3.

29. *Id.*

30. *Id.* art. 19.17.4 (a)–(b).

supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority."[31] In addition to these carve-outs, Article 19.17.5 has subjected the Intermediary Immunity clause to Annex 19-A, which exempts Mexico from its application until the date of three years after the USMCA becomes effective and makes clear its relationship between domestic laws, stating that Mexico will comply with Article 19.17.3 "in a manner that is both effective and consistent with Mexico's Constitution."[32] Further, Annex 19-A clarifies the role of "public morals" under Article XIV of the General Agreement on Trade in Services (GATS) and USMCA Article 32.1.[33]

The Japan-U.S. DTA, too, features the Intermediary Immunity clause in Article 18, copied nearly verbatim from Article 19.17 of USMCA, as the Trump Administration saw this as a "comprehensive and high standard" aligning with rules set by the USMCA.[34] Therefore, the major difference between the Japan-U.S. DTA and USMCA here is one of formality: the commitment to the immunity provision is qualified by a Side Letter clarifying how it interacts with Japan's domestic legal system.[35] The Side Letter reads in relevant part that:

> The Parties recognize that there are differences between their respective legal systems governing the liability of interactive computer services suppliers. The Parties agree that the *Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders* (Law No. 137 of 2001) of Japan is not inconsistent with Article 18 (Interactive Computer Services). Moreover, based on a review of information on the operation of Japan's legal system and discussion between the Parties, the Parties agree that Japan need not change its existing legal system, including laws, regulations, and judicial decisions, governing the

31. *Id.* art. 19.17.4 (c).

32. CPTPP, *supra* note 2,Annex 19-A.1-3.

33. *Id.* Annex 19-A.4.

34. CATHLEEN D. CIMINO-ISAACS & BROCK R. WILLIAMS, CONG. RSCH. SERV., IF11120, JAPAN-U.S. TRADE AGREEMENT NEGOTIATIONS (Dec. 18, 2020).

35. Japan-U.S. Digital Trade Agreement: Side Letter on Interactive Computer Services (Oct. 7, 2019) [hereinafter Japan-U.S. Side Letter]. Although this Side Letter has largely canceled the effect of Japan's commitments under Japan-U.S. DTA Article 18. *See* discussion *infra* Part II.3(c).

> liability of interactive computer services suppliers, to comply with Article 18.[36]

Two additional questions arise here. First, what is the scope of application of the Intermediary Immunity clause—who could benefit from this provision? What exactly does this clause immunize? This turns on our second question: how, if any, this immunity clause affects the policy space of countries in governing online speech? The best way to unfold these issues is perhaps to read the Intermediary Immunity clause within the context of CDA 230, upon which this clause is modeled.

B. *Anatomy of the Intermediary Immunity Clause: A Contextual Analysis*

1. The Intent of Intermediary Immunity Clause and CDA 230

In the USMCA and the Japan-U.S. DTA, the purpose of the Intermediary Immunity clause is merely an economic one: "the promotion of interactive computer services, including for small and medium enterprises, as vital to the growth of digital trade."[37] While this new provision seems straightforward by concentrating on online economic activities, its normative implications for a nation can be sweeping because it touches upon how policymakers balance competing interests of all stakeholders involved, including fundamental rights like freedom of speech. This can be better illustrated through the legislative history of CDA 230.[38] Among others, CDA 230 (c)(1) reads: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[39] This sentence is dubbed as "the twenty-six words that created the Internet" and grew out of a complex history of how the U.S. policymakers balanced competing interests while bolstering the then-nascent Internet as a medium and a marketplace.[40] The legislative

36. *Id.*

37. See USMCA, *supra* note 2, art. 19.17.1; see also Japan-U.S. DTA, *supra* note 4, art. 18.1.

38. The U.S. Congress passed the CDA with the original intention to protect children from harmful materials posted online. While much of this legislation was soon struck down by the Supreme Court on constitutional grounds, CDA 230 survives. Senator Exon, who proposed the CDA, has commented that "the information superhighway should not become a red-light district. This legislation will keep that from happening and extend the standards of decency which have protected telephone users to new telecommunications devices." See 141 CONG. REC. S1953 (daily ed. Feb. 1, 1995).

39. 47 U.S.C.A., § 230 (c)(1).

40. JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019) [hereinafter KOSSEFF, TWENTY-SIX WORDS].

intent was made clear under subsections (a) and (b).[41] In particular, CDA 230(b) enumerates five policy goals, and of these, the first two are in line with those seen in the USMCA and the Japan-U.S. DTA: CDA 230 aims to "promote the continued development of the Internet and other interactive computer services and other interactive media" and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[42] However, the remaining three objectives of CDA 230 go beyond the USMCA and Japan-U.S. DTA by also emphasizing other aspects that equip individuals and service providers with the ability to block illegal contents and considering the need of law enforcement:

> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services; (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.[43]

These enumerated goals were essentially Congress' response to the growing concerns about two landmark judgments in the 1990s: *Cubby v. ComputServe* (*Cubby*) and *Stratton Oakmont v. Prodigy* (*Stratton Oakmont*).[44] Central to these decisions are the debates around freedom of speech guaranteed by the First Amendment to the U.S. Constitution.[45] Traditionally, in the offline context, the U.S. courts adopt different standards in determining liabilities attached to a "publisher" and "distributor" concerning defamatory materials to give effect to the First

41. 47 U.S.C.A. § 230 (a)–(b) (2018).

42. *Id.*

43. *Id.*

44. See Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); see also Stratton Oakmont, Inc., v. Prodigy Servs. Co., 1995 WL 323710, at *4 (N.Y. Sup. May 25, 1995), superseded by statute as stated in Shiamili v. Real Estate Grp. of N.Y., Inc., 929 N.Y.S. 2d 19 (N.Y. 2011).

45. The First Amendment states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." See U.S. CONST. amend. I.

Amendment.[46] While both do not create materials, publishers are, as illustrated in *Smith v. California*,[47] subject to a stricter standard, because they have editorial control over the content while distributors do not.

Entering the Internet age, this analytical framework distinguishing between a "publisher" and "distributor" has faced new challenges. In *Cubby*, an online platform called CompuServe was sued by another company, Cubby, who alleged that materials available on CompuServe's bulletin defamed it.[48] The court rejected this claim and held CompuServe as a distributor with no editorial control over third-party content: the court made clear that CompuServe was liable only if it "knew or had reason to know" of the allegedly defamatory materials.[49] However, not long after this decision, the New York Supreme Court in *Stratton Oakmont v. Prodigy* came out the other way. This case involved an unknown user of Prodigy's online bulletin posting statements indicating that Stratton Oakmont and its staff had committed criminal and fraudulent acts.[50] The court opined that Prodigy was akin to a publisher rather than a distributor because it utilized technologies and workforce to moderate the message boards.[51]

---

46. FOLKERT WILMAN, THE RESPONSIBILITY OF ONLINE INTERMEDIARIES FOR ILLEGAL USER CONTENT IN THE EU AND THE US 98 (2020).

47. In Smith v. California, the U.S. Supreme Court struck down a Los Angeles city ordinance that penalized the possession of obscene materials in places where books were sold. As the bookseller in this case had no knowledge of the criminal activity, imposing such a liability would require it to self-censor the contents of the books. The Court held therefore that "[e]very bookseller would be placed under an obligation to make himself aware of the contents of every book in his shop . . . . And the bookseller's burden would become the public's burden, for by restricting him the public's access to reading matter would be restricted." See Smith v. California, 361 U.S. 147 (1959). Later in 1964, the Supreme Court in the famous case *New York Times v. Sullivan* held that the same logic holds true for liabilities under civil law, as the fear of the recovery of damages can have chilling effects on freedom of speech. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964).

48. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. at 137.

49. *Id.* at 140 ("A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information. Given the relevant First Amendment considerations, the appropriate standard of . . . is whether it knew or had reason to know of the allegedly defamatory Rumorville statements.").

50. Stratton Oakmont, Inc., v. Prodigy Servs. Co., 1995 WL 323710, at *4 (N.Y. Sup. May 25, 1995).

51. The court pointed out Prodigy distinguished itself from ComputServe on two fronts. First, Prodigy "held itself out to the public and its members as controlling the content of its computer bulletin boards" and second, Prodigy "implemented this control through its automatic software screening program, and the Guidelines which Board Leaders are required to enforce." The court thus concluded that Prodigy, by "actively utilizing technology and manpower to delete notes from

Together, these two decisions created the "Moderator's Dilemma" for intermediaries: they are safe by taking a hands-off approach to third-party content, and they will face more legal risks if they take some steps to moderate such content but fail to screen out all harmful information.[52] This result was criticized as "odd" or "absurd,"[53] thus leading Congress to introduce CDA 230 in 1996. The Conference Report concerning this section states:

> One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.[54]

However, the aim of CDA 230 is more than reversing the *Stratton Oakmont* opinion. Congress seized the opportunity to advance five policy objectives, which come down to three themes: first, to prevent harmful online content; second, to promote freedom of expression and information access; and finally, to help the burgeoning Internet and e-commerce flourish.[55]

---

its computer bulletin boards on the basis of offensiveness and 'bad taste'," has made decisions as to contents which constitute editorial control. *Id.*

52. *See, e.g.*, Matthew C. Siderits, *Defamation in Cyberspace: Reconciling Cubby, Inc. v. CompuServe, Inc. and Stratton Oakmont v. Prodigy Services Co.*, 79 MARQ. L. REV. 1065, 1079-80 (1996) (arguing that following these two judgments "it is likely that most major commercial online services will be faced with difficult choices . . . it might choose to take a totally hands-off approach in order that it appear to have no editorial control whatsoever, so as to fall under the auspices of a distributor rather than a publisher."); *see* Goldman, *An Overview of Section 230*, *supra* note 52, at 157-58 (describing the dynamics of these cases as creating the "Moderator's Dilemma").

53. *See* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway,* 49 FED. COMM'N L. J. 52, 61 (1996) ("*Stratton*. . .was the war cry of this absurdity. . ."); see Jeff Kosseff, *The Gradual Erosion of the Law That Shaped the Internet: Section 230's Evolution over Two Decades*, 18 COLUM. SCI. & TECH. L. REV. 1, 6 (2016) (noting that these two decisions had "odd impacts of immunizing online service providers from liability.") [hereinafter Kosseff, *Section 230's Evolution*].

54. H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.).

55. *See* Joris van Hoboken & Daphne Keller, *Design Principles for Intermediary Liability Laws*, Santa Monica Session of the Transatlantic High-Level Working Group on Content Moderation Online and Freedom of Expression 2-3 (2019), https://www.ivir.nl/publicaties/download/Intermediary_liability_Oct_2019.pdf.

In contrast, the USMCA and the Japan-U.S. DTA, as trade agreements, justify the inclusion of the Intermediary Immunity clause on the ground that economic growth and innovation link to "digital trade." Naturally, these immunity clauses in the PTAs omit the terms like "publisher," "speaker," or "whether or not such material is constitutionally protected." In doing so, these trade agreements ostensibly downplay the concerns over relevant parties' policy space in regulating online speech by making this immunity clause look like just another mechanism to facilitate digital trade.

Although the Intermediary Immunity clause spells out its goal as seemingly trade-oriented without references seen in CDA 230(b)(3)-(5), its structure and texts could touch upon the substantive issues revealed in them; Article 19.17.4 USMCA, for instance, clarifies that the immunity will not affect "a Party from enforcing any criminal law."[56] Therefore, despite noticeable textual differences in respect of the underlying objectives under CDA 230 and its comparable Intermediary Immunity clause in the USMCA and the Japan-U.S. DTA, the clause may take a bite out of the policy space available for relevant parties, as discussed below.

2. The Structure of Intermediary Immunity Clause and CDA 230

Structurally, CDA 230 comprises six subsections while the USMCA and the Japan-U.S. DTA have four paragraphs.[57] Having stated the underlying rationales in subsections (a) and (b), CDA 230 in sub-section (c), under the title of "Protection for Good Samaritan," lays down the operative provision to create immunity for disseminating material created by third parties, which reads:

> (1) Treatment of publisher or speaker
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil liability
> No provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable,

56. USMCA, *supra* note 2, art. 19.17.4.

57. *Id.* art. 19.17; see Japan-U.S. DTA, *supra* note 4, art. 18; see 47 U.S.C.A. § 230 (2018).

> whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[58]

From this, several points follow. First and foremost, the immunity of CDA 230 generally applies to "civil liabilities" only with five exceptions outlined under CDA 230 (e).[59] Second and conceptually, CDA 230(c)(1) is concerned with an intermediary's alleged *under-filtering* (*i.e.,* liabilities arising from an intermediary's failure to police harmful third-party content), while CDA 230(c)(2) focuses on cases allegedly involving an intermediary's *over-filtering* (*i.e.,* liabilities resulting from an intermediary's moderating too much by error).[60] Both provisions aim to resolve the Moderator's Dilemma seen in the pre-CDA 230 era; the former immunizes intermediaries that take the hands-off approach to moderate third-party contents, and the latter allows them to be hands-on without risks.[61] Though receiving less attention, the latter is the key driver behind this statute—to overrule the *Stratton Oakmont* decision.[62]

It follows from the above that while none of the comparable provisions under the USMCA and the Japan-U.S. DTA spell out what "liabilities" are immunized explicitly, the reading of CDA 230 reveals what trade negotiators had in mind: this new clause mechanism applies to civil liabilities only.[63] More specifically, Articles 19.17.2 and 19.17.3 of

58. 47 U.S.C.A. § 230 (c)(1) (2018).

59. In short, CDA 230 cannot be used to dismiss a federal criminal prosecution or any lawsuit brought under IPR laws, state laws that are consistent with CDA 230, certain electronic communication privacy laws, or certain sex trafficking laws. There has been controversy surrounding the criminal prosecutions: but while many plaintiffs argued that in cases where the same conduct gave rise to criminal and civil liabilities, allowing CDA 230 to bar suits under a civil enforcement would "impair the enforcement" of the criminal law, such views are rejected by courts. Courts have read CDA 230 (e)(1) to apply to only criminal prosecutions, not civil claims arising from the violation of federal criminal laws. *See* VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 24–25 (2021), https://crsreports.congress.gov/product/pdf/R/R46751#.

60. Doe v. GTE Corp., 347 F.3d 655, 659 (7th Cir. 2003) ("Removing the risk of civil liability may induce web hosts and other informational intermediaries to take more care to protect the privacy and sensibilities of third parties."); WILMAN, *supra* note 46, at 104.

61. WILMAN, *supra* note 46, at 104.

62. Kosseff, *Section 230's Evolution*, *supra* note 53, at 8–9.

63. Some may argue that a plain reading of the Intermediary Immunity clause seems to suggest that its scope could go beyond civil liabilities. Article 19.17.2 of USMCA and Article 18.2 of Japan-U.S.DTA simply refer to "no Party shall adopt or maintain measures that treat. . ..in determining liability for harms related to information stored, processed, transmitted. . ." and Article 19.17.3 of USMCA and Article 18.3 of Japan-U.S. DTA likewise mention only "No Party

USMCA and Articles 18.2 and 18.3 of Japan-U.S. DTA —comparable to CDA 230 (c)(1) and (c)(2)—immunize online platforms' civil liabilities for being hands-off and hands-on towards third-party generated contents.[64]

Relevant carve-outs (*e.g.*, not to be read as affecting a state's enforcement of criminal laws) also provide evidence of civil liability immunity. CDA 230(d) requires intermediaries to make users aware of parental control mechanisms that can be used to restrict access to harmful materials; there is no equivalent under the USMCA or the Japan-U.S. DTA.[65] More crucial are the exceptions under CDA 230(e), which explicitly excludes immunity for the following cases: (i) federal criminal laws;[66] (ii) IPR laws;[67] (iii) any state laws that are consistent with CDA 230;[68] (iv) the Electronic Communications Privacy Act of 1986,[69] and (v) civil actions or state prosecutions where the alleged conduct breaches relevant federal laws concerning sex trafficking.[70] USMCA and Japan-U.S. DTA likewise have carve-outs, albeit differently worded. For instance, USMCA Article 19.17.4 states that this provision shall not:

---

shall impose liability on a supplier or user of an interactive computer service on account of. . .." The term "liability" is defined by Oxford Dictionary as "the state of being legally responsible for something." *See* Oxford Learner's Dictionaries, https://www.oxfordlearnersdictionaries.com/definition/english/liability?q=%22liability%22. However, a contextual interpretation by considering the exceptions under Article 19.17.4 of USMCA and Article 18.4 of Japan-U.S. DTA (*e.g.,* "Nothing in this Article shall (c) be construed to prevent (i) a Party from any criminal law, or. . . "a supplier or use of an interactive computer service from complying with a specific, lawful order of a law enforcement authority.") and its origin—CDA 230, indicate that this new provision provides the legal shield for civil liabilities. This reading can be supported by the Side Letter of the Japan-U.S. DTA, which contains the reference to the Law No. 137/2001—one that addresses the limitation of civil liabilities.

64. USMCA, *supra* note 2, art. 19.17.2–.3; Japan-U.S. DTA, *supra* note 4, art. 18.2 and 18.3. In the CDA 230 context, the US courts have read the exception for laws "pertaining to intellectual property law" under CDA 230 (e) (2) to allow for lawsuits based on copyright and trademark infringement. This may shed light on the interpretation of the scope of immunity CDA-230 comparable clauses under USMCA and Japan-U.S. DTA.

65. 47 U.S.C.A. § 230 (d) (2018).which reads: "A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections."

66. 47 U.S.C.A. § 230 (e)(1) (2018).

67. *Id.* § 230 (e)(2).

68. *Id.* § 230 (e)(3).

69. *Id.* § 230 (e)(4).

70. *Id.* § 230 (e)(5).

> (a) apply to any measure of a Party pertaining to intellectual property, including measures addressing liability for intellectual property infringement; or (b) be construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right; or (c) be construed to prevent: (i) a Party from enforcing any criminal law, or (ii) a supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority.[71]

Further, the USMCA and the Japan-U.S. DTA both condition the Intermediary Immunity clause on specific qualifications under the Annex and Side Letter, respectively.[72] Finally, CDA 230(f) offers definitions of relevant terms, and analogous provisions can be found under Article 19.1 USMCA and Article 1 Japan-U.S. DTA.[73] To further our understanding of the potential implications of the Intermediary Immunity clause for global trade, the section that follows places the analysis within a comparative context by narrowing our focus on CDA 230 (c) and (e) and their comparable ones in the USMCA and the Japan-U.S. DTA.

3. A Deep Dive Reading of CDA 230 and Intermediary Immunity Clause

Central to CDA 230 is subsection (c), which inspires trade negotiators in designing the comparable provisions in USMCA and Japan-U.S. DTA. Textual similarities have led some leading experts in CDA 230 to read the Intermediary Immunity clause as conferring similar protections as CDA 230.[74] To illustrate this, a good starting point is to examine key terminologies exported from CDA 230 to USMCA and Japan-U.S. DTA.

The USMCA and Japan-U.S. DTA borrow from CDA 230 major terminology, including "interactive computer service" and "information content provider."[75] Such borrowing is of normative value. CDA 230(c)(1) immunizes only providers (or users) of interactive computer service rather than information content providers. The former is defined by

71. USMCA, *supra* note 2, art. 19.17.4; *see also* Japan-U.S. DTA, *supra* note 4, art. 18.4.

72. USMCA, *supra* note 2, art. 19.17.5; Japan-U.S. Side Letter, *supra* note 35.

73. USMCA, *supra* note 2, art. 19.1; Japan-U.S. DTA, *supra* note 4, art. 1.

74. *See* Eric Goldman, *Good News! USMCA (a/k/a NAFTA 2.0) Embraces Section 230-Like Internet Immunity*, TECH. & MARKETING L. BLOG (Oct. 8, 2018), https://blog.ericgoldman.org/archives/2018/10/good-news-USMCA-a-k-a-nafta-2-0-embraces-section-230-like-internet-immunity.htm [hereinafter Goldman, *Good News*].

75. USMCA, *supra* note 2, art. 19.1; Japan-U.S. DTA, *supra* note 4, art. 1.

CDA 230 as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions" while the latter denotes "any person or entity that is responsible, in whole or in part, for the creation or development of information."[76] The U.S. courts have read interactive computer service providers as broadly including "virtually any services available through the internet."[77] Online marketplace,[78] social media operators,[79] blogging sites,[80] search engines,[81] consumer rating platforms,[82] and online dating service providers are prime examples.[83]

In comparison, USMCA Article 19.17.2 and Japan-U.S. DTA Article 18.2 likewise apply only to suppliers or users of "interactive computer services"—a term with a similar yet shorter definition compared to its comparable definition under CDA 230.[84] Arguably, a variety of the U.S. high-tech firms—including Big Tech—can take advantage of it if this term can be interpreted as broadly at the international level as seen in the U.S. context. Notably, USMCA Article 19.17.2 and Japan-U.S. DTA Article 18.2 further clarify that they are not applicable where "the supplier or user has, in whole or in part, created, or developed the information."[85] This qualification appears somehow redundant because any person who "creates or develops, in whole or in part, information provided through the Internet or another interactive computer service" already falls within the scope of "information content provider" under the USMCA and the Japan-U.S. DTA, and therefore, is not entitled to

76. USMCA, *supra* note 2, art. 19.17.2; Japan-U.S. DTA, *supra* note 4, art. 18.2.

77. Goldman, *An Overview of Section 230*, *supra* note 52, at 159–60.

78. *See, e.g.*, Dart v. Craigslist, Inc., 665 F. Supp. 2d 961 (N.D. Ill. 2009); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703 (Ct. App. 2003).

79. *See* Caraccioli v. Facebook, Inc., 700 F. App'x 588, 589-90 (9th Cir. 2017) (holding that Facebook was not an information content provider under Section 230(c)(1)).

80. *See* Bennett v. Google, LLC, 882 F.3d 1163 (2018).

81. *See, e.g.*, Goddard v. Google, Inc., 640 F. Supp. 2d 1193 (N.D. Cal. 2009); see Jurin v. Google, Inc., 695 F.Supp. 2d 1117 (E.D. Cal. 2010).

82. *See* Reit v. Yelp!, Inc., 907 N.Y.S.2d 411, 412 (Sup. Ct. 2010).

83. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).

84. *Id.* at 1123–24.

85. USMCA, *supra* note 2, art. 19.1; Japan-U.S. DTA, *supra* note 4, art. 1.

this immunity.[86] This qualification is of little help to address a recurring problem in the CDA 230 jurisprudence—how could an intermediary not overly moderate third-party content in a way that turns itself into more than a mere conduit for expression, thus losing its immunity? Where should the line be drawn between "interactive computer services" and "information content provider"?

Of relevance to this problem are the footnotes added in USMCA Article 19.17.2 and Japan-U.S. DTA Article 18.2, which state, respectively: "For greater certainty, a Party may comply with this Article through its laws, regulations, or application of existing legal doctrines as applied through judicial decisions."[87] It follows that, for the U.S. part at least, the "material contribution" standard of review established by the case law remains the key to distinguish interactive computer service and information content providers.[88]

Second, USMCA Article 19.17.3 and Japan-U.S. DTA Article 18.3 are analogous to CDA 230(c)(2). As noted above, these provisions are set to immunize intermediaries adopting a hands-on approach towards third-party content; by contrast, Article 19.17.2 USMCA and Article 18.2 Japan-U.S. DTA protect those being hands-off. The function of these two CDA 230(c)(2)-like clauses is—although not explicitly spelled out as CDA 230(b)(3)-(4) mentioned above—to remove disincentives for intermediaries to moderate content.

Further, the immunity under USMCA Article 19.17.3 and Japan-U.S. DTA Article 18.3 is granted only on one of the two specified grounds. First, an intermediary acts in "good faith" by removing the content that it considers to be "harmful or objectionable."[89] Second, an intermediary provides technical means (*e.g.,* anti-malware) for others to block the

86. USMCA, *supra* note 2, art. 19.1; Japan-U.S. DTA, *supra* note 4, art. 1. Under both provisions, "information content provider" refers to "a person or entity that creates or develops, in whole or in part, information provided through the Internet or another interactive computer service."

87. USMCA, *supra* note 2, art. 19.17.2; Japan-U.S. DTA, *supra* note 4, art. 18.2.

88. *See, e.g.,* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1167–68 (9th Cir. 2008) (holding that the intermediary is liable if it "not merely to augment the content generally, but to materially contribute to its alleged unlawfulness."). Some commentators further suggested that the "created or developed" qualifications in the USMCA "codifies the 'material contribution' standard as established by the U.S. Ninth Circuit Court of Appeals in the *Roommates.com* case." *See* Krishnamurthy & Fjeld, *CDA 230 Goes North American*, *supra* note 6, at 6. However, this claim seems to go too far, as the footnotes inserted in Articles 19.17.2 USMCA and Article 18.2 Japan-U.S. DTA have left relevant parties to determine how it can be interpreted as per their respective domestic laws and jurisprudence.

89. USMCA, *supra* note 2, art. 19.17.3 (a); Japan-U.S. DTA, *supra* note 4, art. 18.3 (a).

above contents.[90] Of particular note is the first one. While CDA 230(c)(2)(A) refers to the content in dispute that should be "obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected,"[91] USMCA Article 19.17.3 (a) and Japan-U.S. DTA Article 18.3 (a) require the content to be "harmful or objectionable."[92] By way of a general term, the Intermediary Immunity clauses in the USMCA and Japan-U.S. DTA avoid the potential debates that occurred in the CDA 230 jurisprudence: whether the "harmful or objectionable" content should be read per the *ejusdem generis* rule, and thus, should be related to "obscene, lewd, filthy, excessively violent, or harassing."[93] In this light, USMCA and Japan-U.S. DTA seem to be friendlier to high-tech firms than CDA 230 (c)(2)(A).

Moreover, the inclusion of "harmful or objectionable," suggests that the illegality of the content is not the prerequisite for this immunity; an intermediary will not make its liability shield unavailable even if it removes manifestly illegal user content.[94] Further expanding the scope of immunity is the term "it considers," meaning that harmfulness or objectionableness is subject to an intermediary's judgment call.[95] The only limit to restrain intermediaries' discretion in moderating content is the "good faith" requirement in USMCA Article 19.17.3 (a) and Japan-U.S. DTA Article 18.3 (a). The precise contour of the "good

90. USMCA, *supra* note 2, art. 19.17.3 (b); Japan-U.S DTA, *supra* note 4, art. 18.3 (b).

91. 47 U.S.C.A. § 230 (c)(2)(A) (2018).

92. USMCA, *supra* note 2, art. 19.17.3 (a); Japan-U.S. DTA, *supra* note 4, art. 18.3 (a).

93. *See, e.g.,* Nat'l Numismatic Certification, LLC. v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL2704404, at *23–26 (M.D. Fla. July 8, 2008) ("One may find an array of items objectionable . . . However, Congress provided guidance on the term "objectionable" by providing a list of seven examples and a statement of the policy behind section 230. Accordingly, the Court concludes that "objectionable" content must, at a minimum, involve or be similar to pornography, graphic violence, obscenity, or harassment."). The ejusdem generis principle has also been applied by the WTO adjudicators. *See, e.g.*, Appellate Body Report, *United States–Certain Country of Origin Labelling (COOL) Requirements*, ¶¶ 443–44, WTO Doc. WT/DS384/AB/R, WT/DS386/AB/R (adopted June 29, 2012).

94. *See* WILMAN, *supra* note 46, at 116.

95. In a similar yet separate context, the references to "it considers" can also be found in the WTO regime. Notably, the "national security" exceptions under Article XXI of the GATT provides that "Nothing in this Agreement shall be construed. . .(b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests." The phrase "it considers" has become a subject of debate as to whether this clause is a self-judging one—and its justiciability. On this score, see, e.g., Daria Boklan & Amrita Bahri, *The First WTO's Ruling on National Security Exception: Balancing Interests or Opening Pandora's Box?* 19 WORLD TRADE REV. 123 (2020); Roger P. Alford, *The Self-Judging WTO Security Exception*, 2011 UTAH L. REV. 697.

faith" element remains to be seen at the international level through adjudication or negotiation processes, although this element is not a significant hurdle to overcome in the CDA 230 jurisprudence.[96] Together, the potential breadth of immunity granted in Article 19.17.3 USMCA and Article 18.3 Japan-U.S. DTA can be sweeping, which could arguably narrow the regulatory space of relevant parties to govern online speech, as discussed further below.

C. *The Normative Impacts of The Intermediary Immunity Clause*

While the drafters attempted to downplay the concerns about regulating online intermediaries by using the seemingly innocuous title "Interactive Computer Services" in the USMCA and the Japan-U.S. DTA, our contextual analysis has revealed non-economic concerns—like freedom of expression—embedded in this clause. Much of what is blamed for the losing policy space of online speech is of dubious merit: is it online intermediaries or governments, or both, that can shape the normative order of the Internet after a nation accepts the Intermediary Immunity clause? Before unpacking the relevant ramifications, it is crucial to first further clarify the scope of the legal shield of this CDA 230-like provision in the trade agreements.

1. Clarifying the Scope of Liabilities

The primary effect of the Intermediary Immunity clause is that it helps encourage online intermediaries' development and expansion of their businesses by increasing their confidence through not holding them liable if a user on their platforms violates the rights of others. Specifically, by "liabilities," the Intermediary Immunity clause applies only to "civil" claims concerning third-party content or for the removal of content under some circumstances.[97] Arguably, some commentators point to the textual difference between CDA 230(c) and USMCA Article 19.17.2, suggesting that CDA 230 bars *all* actions (statutory or

96. *See, e.g.*, Eric Goldman, *Online User Account Termination and 47 U.S.C. § 230(c)(2)*, 2 U.C. IRVINE L. REV. 659, 665 (2012) [hereinafter Goldman, *Online User Account Termination*]; see WILMAN, *supra* note 46, at 116 (noting that in recent years, there are several court decisions reading this term more narrowly). Note however that, in contrast with Article 19.17.2 USMCA and Article 18.2 Japan-U.S. DTA, no footnotes are added to Article 19.17.3 USMCA and Article 18.3 Japan-U.S. DTA to allow relevant parties to defer to their domestic laws and jurisprudence in compliance with these provisions.

97. *See* Mark Lemley, *Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101 (2007).

common law), while the Intermediary Immunity clause only explicitly refers to the former, leaving open the possibility of equitable relief.[98]

To be clear, per USMCA Article 19.17.4 and Japan-U.S. DTA Article 18.4, the legal shield does not apply to IPR infringement, nor does it affect criminal law enforcement.[99] In respect of IPR infringement, the U.S. has already exported rules on intermediaries' liabilities and the so-called "Safe Harbors" that emulate its DMCA to other countries through trade,[100] such as the U.S.-Chile FTA,[101] the U.S.-Singapore FTA,[102] and the U.S.-Australia FTA,[103] and more recently, CPTPP and USMCA.[104] USMCA Article 20.88, for instance, obligates Parties to "ensure that legal remedies are available for right holders to address [online] copyright infringement and establish or maintain appropriate safe harbors [for] Internet Service Providers."[105] The safe harbor under the USMCA IPR chapter immunizes online intermediaries for copyright infringements which "they do not control, initiate or direct."[106] Two issues are noteworthy. First, the DCMA-type safe harbor generally applies to copyright infringement,[107] while the Intermediary Immunity clause uses generic terms, such as "intellectual property" and "intellectual property right," when referring to what falls outside of it.[108] Second, and more crucially, unlike the Intermediary Immunity clause, the DMCA-type safe harbor is qualified by the "notice and takedown" element; intermediaries must expeditiously remove or disable access to the infringing content "upon obtaining actual knowledge" or

98. Krishnamurthy & Fjeld, *CDA 230 Goes North American*, *supra* note 6, at 6.

99. USMCA, *supra* note 2, art. 19.17.4 (a)–(c); Japan-U.S. DTA, *supra* note 4, art. 18.4. (a), (b), and (c).

100. *See generally* Andrew Christie et al., *Exporting the DMCA through Free Trade Agreements*, *in* INTELLECTUAL PROPERTY AND FREE TRADE AGREEMENTS 211 (Christopher Heath & Anselm Kamperman Sanders eds., 2007). CDA 230 and the DMCA are two of the three U.S. federal statutes that offer limited liabilities for online intermediaries. The third one yet less known is the Lanham Act, 15 U.S. C. § 1114(2)(B), (C) (2006).

101. United States-Chile Free Trade Agreement, Chile-U.S., June 6, 2003, State Dept. No. 04-35, 2003 WL 23856180, https://ustr.gov/trade-agreements/free-trade-agreements/chile-fta [hereinafter *U.S.-Chile FTA*].

102. United States-Sing. Free Trade Agreement, May 6, 2003, https://ustr.gov/trade-agreements/free-trade-agreements/singapore-fta [hereinafter *U.S.-Singapore FTA*].

103. United States-Austl. Free Trade Agreement, May 18, 2004, https://ustr.gov/trade-agreements/free-trade-agreements/australian-fta [hereinafter *AUSFTA*].

104. CPTPP, *supra* note 2, art. 18.82; USMCA, *supra* note 2, art. 20.88.

105. USMCA, *supra* note 2, art. 20.88.

106. *Id.* art. 20.88.1 (b).

107. In the U.S., Section 32(2) of the Lanham Act creates a form of safe harbor for trademark infringements. See Lemley, *supra* note 97, at 107–08.

108. *See, e.g.*, USMCA, *supra* note 2, art. 19.17.4 (a)–(b).

"becoming aware of" the infringement.[109] Hence, the absence of this notice-and-take-down requirement makes the legal shield under the Intermediary Immunity clause far more generous than what the DMCA-analogous safe harbor has promised.

Turning to criminal enforcement, intriguingly, the Intermediary Immunity clause seems to leave more space for nations to craft their domestic policies. CDA 230 primarily pierces the shield for federal criminal prosecution,[110] while its analogous arrangements in the USMCA and the Japan-U.S. DTA,[111] with references to only "any criminal law," exempt all criminal charges, regardless of their level.[112]

What remains unclear is how the Intermediary Immunity clause applies when it shall not be construed to prevent "a supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority."[113] This exemption, if interpreted broadly in conjunction with other qualifications under the USMCA Annex 19-A, Side Letter of the Japan-U.S. DTA, and relevant footnotes, might make the Intermediary Immunity clauses less worrying than it appears to be, as discussed below.

2. ONLINE Platforms as the New Global Ruler of Internet Speech in the Post-Intermediary Immunity Clause Era?

The broad immunity under USMCA Article 19.17 could be worrisome because it could arguably move intermediaries, rather than governments, to the center of regulating online speech. The Intermediary Immunity clause's normative implications are evident if we place it within the real-world context. For example, anyone in Japan who wishes to join their approximately 51 million fellow Japanese Twitter users

109. *Id.* art. 20.88.1 (a).

110. 47 U.S.C.A. § 230 (e)(1) (2018). However, the most recent amendment to CDA 230—known as "Allow States and Victims to Fight Online Sex Trafficking Act of 2017" (FOSTA)—has removed CDA immunity for online platforms concerning state criminal charges if the conduct underlying the state violation would constitute a violation of the anti sex-trafficking statutes outlined in the FOSTA. *See also* 47 U.S.C.A. § 230 (e)(5) (2018).

111. A '*Limitations on Liability for Internet Service Providers'* is set out in the following agreements. *See Australia-US Free Trade Agreement,* Austl-U.S., art 17.11.29, signed May 18 2004, [2005] A.T.S 1 (entered into force Jan. 1, 2005); *see United States-Singapore Free Trade Agreement,* S*ing* -U.S.,, art .16.9.22, signed May 6, 2003, [2004] (entered into force Jan. 1, 2004); see *United States-Chile Free Trade Agreement,* C*hile* -U.S., art. 17.11.23 [2004] (entered into force Jan. 1, 2004); see *United States-Colombia Trade Promotion Agreement, Colom*-U.S., art. 16.11.29, signed Nov. 22, 2006, [2012] (entered into force May 15, 2012); *see United States-Bahrain Free Trade Agreement*, Bahrain-U.S., art. 14.10.29 [2006] (entered into force Jan. 11, 2006).

112. USMCA, *supra* note 2, art. 19.17.4 (c)(i); Japan-U.S. DTA, *supra* note 4, art. 18.4 (c)(i).

113. Id.

must "agree to form a binding contract with Twitter" with the terms and conditions specified on its platform. [114] Part III of the Twitter Terms of Service "Content on the Services" begins by stating that:

> You are responsible for your use of the Services and for any Content you provide, including compliance with applicable laws, rules, and regulations. You should only provide Content that you are comfortable sharing with others.[115]

This contract provision makes clear that users are bound by their contracts with Twitter and applicable laws in Japan for whatever content they post on this social media. Twitter then states explicitly in the contract that it assumes no liabilities for the users' content:

> Any use or reliance on any Content or materials posted via the Services or obtained by you through the Services is *at your own risk*. We do not endorse, support, represent or guarantee the completeness, truthfulness, accuracy, or reliability of any Content or communications posted via the Services or endorse any opinions expressed via the Services. You understand that by using the Services, *you may be exposed to Content that might be offensive, harmful, inaccurate or otherwise inappropriate, or in some cases, postings that have been mislabeled or are otherwise deceptive. All Content is the sole responsibility of the person who originated such Content*. We may not monitor or control the Content posted via the Services and, we cannot take responsibility for such Content.[116]

Through its contracts, Twitter seeks to protect itself from potential liabilities by *under-filtering* harmful content. While this part allows Twitter to take a hands-off approach towards third-party content, the next paragraph goes further, allowing Twitter to actively moderate content:

> *We reserve the right to remove* Content that violates the User Agreement, including for example, copyright or trademark

114. *Leading Countries Based on Number of Twitter Users as of January 2022*, STATISTA, https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/.

115. *Twitter Terms of Services*, TWITTER (Aug. 19, 2021), https://twitter.com/en/tos [hereinafter *Twitter TOS*]. There is another version of contract for Twitter users who live in the EU, EFTA, or the UK.

116. *Id.*

> violations or other intellectual property misappropriation, impersonation, *unlawful conduct, or harassment.*[117]

The "including for" clause enables Twitter to be hands-on or even over-filter users' content if they see fit. Indeed, Twitter sees itself as a global forum to "serve the public conversation."[118] To safeguard its "value of global public conversation," it aims to fight off "[v]iolence, harassment, and other similar types of behavior" that can discourage freedom of expression.[119] To this end, Twitter articulates a set of policies—known as "Twitter Rules"—governing a range of issues such as violence,[120] terrorism,[121] child sexual exploitation,[122] harassment,[123] and hateful conduct.[124] One immediate observation follows: CDA 230-type provisions in trade agreements could *entrench, rather than diminish*, the power of these social media companies in governing online speech globally.

While social media companies' terms of services (*e.g.*, those of Twitter) often contain a reference to users' compliance with applicable local laws, the CDA-230-like clauses in the USMCA and the Japan-U.S. DTA create new constraints on how relevant parties craft their laws, making such a reference less meaningful. The default rule set by the Intermediary Immunity clause is similar to the contractual arrangement because it shields intermediaries from liabilities for being passive or positive in moderating online content.

As discussed above, USMCA Article 19.17.2 and Japan-U.S. DTA Article 18.2 allow intermediaries to take a hands-off approach without worrying about the liabilities from third-party content unless an intermediary crosses the red line and becomes an "information content

117. *Id.*

118. *Twitter Rules*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-rules#hateful-conduct (last visited Mar. 1, 2022) [hereinafter *Twitter Rules*].

119. *Id.*

120. *Violent Threats Policy*, TWITTER (Mar. 2019), https://help.twitter.com/en/rules-and-policies/violent-threats-glorification.

121. *Violent Organizations Policy*, TWITTER (Oct. 2020), https://help.twitter.com/en/rules-and-policies/violent-groups.

122. *Child Sexual Exploitation Policy*, TWITTER (Oct. 2020), https://help.twitter.com/en/rules-and-policies/sexual-exploitation-policy.

123. *Abusive Behavior*,, https://help.twitter.com/en/rules-and-policies/abusive-behavior (last visited Mar. 1, 2022).

124. *Hateful Conduct Policy*, *Twitter,* https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy (last visited Mar. 1, 2022).

provider."[125] The footnotes inserted into these provisions seem to move the parties to the driver's seat by deference to the local laws and jurisprudence of relevant parties to determine what information content provider means. While this could moderate the concerns over a country's policy space to regulate online speech, it remains to be seen how the footnote will be interpreted in practice. If the term "existing" could be broadly read to inform the reading of "its laws, regulations," this new clause would still affect a party's ability to take new measures. Having qualifications in place—as Japan has done via the Side Letter—would be an option for countries to preserve their policy space. Of course, whether and to what extent can qualifications be made are depending upon the bargaining power and the underlying interests of the relevant parties, as discussed below.

The effect of Article 19.17.3 USMCA and Article 18.3 Japan-U.S. DTA could be problematic for domestic policymakers. Specifically, these CDA 230(c)(2)(A)-like clauses can not only protect intermediaries from liabilities concerning third-party content but immunize their "first-party" filtering decisions—that is, their judgments to moderate or screen out materials, or even ban a user's account if they deem relevant content "harmful or objectionable."[126] This would appear in line with the contractual arrangements set out by those social media firms, as seen in the case of Twitter. As a result, USMCA Article 19.17.3 and Japan-U.S. DTA Article 18.3 would arguably help online intermediaries to go as far as they wish—including censorship—without worrying about private actions in other jurisdictions.[127] There are potential ramifications of this chilling effect. Given their formidable market power

125. As defined under USMCA Article 19.1 and Japan-U.S. DTA Article 1. See USMCA, *supra* note 2, art. 19.1; *see* Japan-U.S. DTA, *supra* note 4, art. 1.

126. WILMAN, *supra* note 46, at 114; Goldman, *Online User Account Termination*, *supra* note 96, at 662.

127. As a matter of contract, users who violate any of these Twitter Rules could lead to account suspension. *About Suspended Accounts, Twitter*, https://help.twitter.com/en/managing-your-account/suspended-twitter-accounts (last visited Mar. 1, 2022). Such a contractual right can be entrenched by adding the Intermediary Immunity clause in trade deals. Adam Candeub, *Commentary: Renegotiated NAFTA Will Entrench Big Tech Censorship,* REALCLEAR POLITICS (NOV. 23, 2018), https://www.realclearpolitics.com/articles/2018/11/23/renegotiated_nafta_will_entrench_big_tech_censorship_138731.html (also arguing that the USMCA, by keeping only "harmful or objectionable" in Article 19.17.3., "would give Big Tech the statutory right to censor whatever content it finds 'objectionable'."). In Japan, however, it is not a big concern for a party to sue Twitter or other social media platforms because of the Side Letter.

resulting from network effects,[128] any filtering decision made by Twitter, Facebook, or other Big Tech firms may have chilling effects on those users who want to stay in the social networks for obvious reasons.[129]

Such concerns are less worrisome in the context of "small and medium enterprises,"[130] another group of beneficiaries protected under the Intermediary Immunity clause, for their lack of market power. In one sense, therefore, because of this chilling effect, countries might leave freedom of speech, a fundamental right which is guaranteed through its enshrinement in Article 19 of the United Nations' Universal Declaration of Human Rights, to the discretion of Big Techs in the name of "digital trade."[131]

This concern is also true for the U.S.; there is longstanding criticism against this robust Intermediary Immunity, and the 2016 and 2020 Presidential elections escalated the controversy to a new level.[132]

128. On the market power of social media, *See, e.g.*, Catherine Tucker, *Digital Data, Platforms and the Usual [Antitrust] Suspects: Network Effects, Switching Costs, Essential Facility*, 54 REV. INDUS. ORG. 683 (2019) (noting that "[n]etwork effects occur when a good or service increases in usefulness with more users. Firms can derive market power from network effects because they imply increasing returns to firm size" and it is harder for smaller firms to compete and attract users); see Tim Stobierski, *What Are Network Effects?*, HARV. BUS. SCHOOL ONLINE (Nov. 12, 2020), https://online.hbs.edu/blog/post/what-are-network-effects (describing social media platforms such as Facebook and Twitter as "heavily influenced by network effects'').

129. *See, e.g.*, Nicole B. Ellison et al., *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites*, 12 J. COMP.-MEDIATED COMM'N. 1143 (2007) (pointing out that there is a strong correlation between Facebook use, the connection to the communities, and the payoffs in terms of jobs, and other opportunities).

130. USMCA, *supra* note 2, art. 19.17.1; Japan-U.S. DTA, *supra* note 4, art. 18.1. Arguably, it would be more difficult for upstarts to compete with the incumbent tech giants without the immunity clause. Elizabeth Nolan Brown, *Section 230 is the Internet's First Amendment. Now Both Republicans and Democrats Want to Take It Away*, REASON, (July 29, 2019), https://reason.com/2019/07/29/section-230-is-the-internets-first-amendment-now-both-republicans-and-democrats-want-to-take-it-away/.

131. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 19 (Dec. 10, 1948).

132. According to one survey, the 2020 US Presidential Election featured "dramatic increases in lawmaker posts and audience engagement." The election campaign itself was, in other words, "much more online than the preceding presidential cycle." See *Charting Congress on Social Media in the 2016 and 2020 Elections*, PEW RESEARCH CENTER (Sept. 30, 2021), https://www.pewresearch.org/politics/2021/09/30/charting-congress-on-social-media-in-the-2016-and-2020-elections/. The role of social media has therefore been under the spotlight of both Democrats and Republicans. Trump attacked CDA 230, as social media platforms labeled the posts they considered misleading or false; Democrat critics attempted to hold "tech companies more accountable for hate speech and extremism." *See e.g.*, Jessica Guynn, *Trump vs. Big Tech: Everything You Need to Know About Section 230 and Why Everyone Hates It*, USA TODAY, (Oct. 16, 2020, 5:43 PM), https://www.usatoday.com/story/tech/2020/10/15/trump-section-230-facebook-twitter-google-conservative-bias/3670858001/.

Mindful of the Intermediary Immunity clause's sweeping impacts, relevant parties have clawed back the power to regulate through various qualifications, thus making the CDA 230-type arrangement less effective than it appears to be.

3. Intermediary Immunity Clauses: All Bark and No Bite?

While the U.S. embedded CDA 230 through trade agreements, the normative implications for Japan, Canada, and Mexico are running on a continuum. At one end of the spectrum lies Japan. Although Japan did not require a grace period (as in the case of Mexico), it did use the Side Letter to effectively cancel much of the effect of the Intermediary Immunity clause. Both parties agree in the Side Letter that Japan's "Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Sender (Law No. 137 of 2001)" is not inconsistent with Article 18 of Japan-U.S. DTA.[133] Therefore, no changes to the existing legal systems are required for the purpose of the Japan-U.S. DTA Article 18.[134]

Intriguingly, there are noticeable differences between Japan's Law 137/2001 and the CDA 230-type clause. First, while the Intermediary Immunity clause's structure is influenced by CDA 230 to tackle the Moderator's Dilemma under the First Amendment, insulating an online intermediary from liabilities for being a passive or active moderator, no such distinction seems to be made in Japan's Law 137/2001.[135] Moreover, Law 137/2001 features the "notice and takedown" approach.[136] In Japan,

133. Japan-U.S. Side Letter, *supra* note 35.

134. *Id.*

135. 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律 Tokutei denkitsuushin ekimu teikyousha no songaibaishou sekinin no seigen oyobi hasshinsha jouhou no kaiji ni kansu ru houritsu [Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers and the Right to Request Disclosure of Identification Information of the Senders], Law No. 137 of 2001, art. 3, translated at UNESCO, http://www.unesco.org/culture/pdf/anti-piracy/Japan/Jp_%20LimitLiability_Telecom_en (last visited Mar. 10, 2022) (Japan) [hereinafter *Japan's Law 137/2001*]. The Law 137/2001 broadly applies to various claims, such as copyright infringement, defamation, privacy intrusion and so on. *See* 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律解説 Tokutei denki tsushin ekimu teikyo-sha no songai baisho sekinin no seigen oyobi hasshinsha joho no kaiji ni kansuru horitsu kaisetsu [Commentary on Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers and the Right to Request Disclosure of Identification Information of the Senders], MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS (Jan. 2017), https://www.soumu.go.jp/main_content/000461787.pdf (Japan).

136. Japan's Law 137/2001, *supra* note 135, art. 3.

an intermediary shall not be liable for any loss incurred from others' rights infringed by information the intermediary distributed,[137] unless (i) it is "technically possible to take measures for preventing such information from being transmitted to unspecified persons," (ii) it knew, or there was "reasonable ground to find that said relevant service provider could know" of the infringement, and (iii) the intermediary transmits the information itself.[138] By imposing not only an actual knowledge-and-takedown approach but a more vague "reasonable ground" that the provider "could know," as Professor Anupam Chander remarks, Japan's 137/2001 Law is "a pale shadow of the CDA Section 230 from the perspective of Internet enterprise."[139] Even more so, the 137/2001 Law is more onerous than CDA 230 by requiring intermediaries to disclose the identity of the defaming poster.[140] Although the Japanese courts have been careful in interpreting intermediaries' liabilities and have considered competing interests,[141] the Side Letter essentially undoes what the Intermediary Immunity clause aimed for in the first place. In short, Japan has qualified the Intermediary Immunity clause by reducing the Intermediary Immunity to have minimal effect, if not eradicated altogether. Japan's Side Letter can therefore moderate some of the concerns about the power of Twitter and other social media platforms as underscored above.

Canada, sitting on the other end of the spectrum, presents an interesting case. It made no reservations like Japan or Mexico, nor does Canada have laws analogous to CDA 230 in the U.S. or 137/2001 Law

137. Japan's Law 137/2001, *supra* note 135, art. 3.

138. *Id.*

139. Anupam Chander, *Internet Intermediaries as Platforms for Expression and Innovation* 5 (CIGI, Global Comm'n on Internet Governance Paper Series No. 42, 2016), https://www.cigionline.org/static/documents/documents/GCIG%20no.42.pdf.

140. Japan's Law 137/2001, *supra* note 135, art. 4.

141. In a landmark decision made in 2010, Japan's Supreme Court read the disclosure requirement narrowly, for disclosing the identity touched upon the privacy, freedom of speech, and the confidentiality of communications of a user. [Sup. Ct.], 発信者情報開示等請求事件（平成21(受)609）Hasshinsha joho kaiji-to seikyu jiken (Heisei 21(jyu) 609) [Sender Information Disclosure Request Case] (Japan), https://www.courts.go.jp/app/files/hanrei_jp/104/080104_hanrei.pdf; see Hiroko Onishi, *The Online Defamation Maze: Are We Finding a Way Out?,* 27 (1-2) INT'L. REV. L., COMP. & TECH. 200, 207 (2013) (arguing that this 2010 decision is "more likely to indicate that the court has shown a cautious view on, and limitation in, imposing liability on the ISPs for damages.").

in Japan.[142] Civil liabilities arising from defamation are primarily addressed through common law.[143] Defamatory liability under Canadian common law is considered by some to be too harsh for online intermediaries, and there are calls for the government to modify it. Professor Michael Geist, a leading Canadian legal scholar, described this new clause as a "welcome addition" to the USMCA that "remedies a long-standing problem in Canada" and helps the nation "build an innovative online economy."[144]

Several immediate observations follow. First, Canada may, but is not obligated to, pass a CDA 230 equivalent.[145] USMCA Article 19.17 cannot be read as imposing a positive duty on Canada to introduce its own CDA 230. As noted earlier, USMCA Article 19.17.2 is qualified by a footnote to allow parties to comply with the Intermediary Immunity clause "through its laws, regulations, or application of existing legal doctrines as applied through judicial decisions."[146] Thus, Canada can comply with its obligation if policymakers refrain from implementing new rules to hold online platforms liable for third-party content and "[leave] it to the courts to reject claims that run counter to the safe harbor principle."[147] This turns on the second, related issue: how to reconcile the tension between Canadian common law and treaty obligations. In

142. *See, e.g.*, Eric Goldman, *Five Things To Know About Section 230,* CENTRE FOR INT'L GOVERNANCE INNOVATION (June 21, 2021), https://www.cigionline.org/articles/five-things-to-know-about-section-230/; see Law Commission of Ontario, DEFAMATION LAW IN THE INTERNET AGE 4 (Final Report, Mar. 2020) (recommending that Ontario *Libel and Slander Act* (LSA) should be repealed and introduce a new *Defamation Act* establishing "an integrated framework for resolving both online and offline defamation in Ontario" and this new law should include a "new takedown remedy for defamation complaints.").

143. *Id.* at 10 ("The substantive elements of defamation law should not be codified but, subject to specific recommendations below, should continue to develop in common law.").

144. Geist, *From Copyright Term to Super Bowl Commercials*, supra note 6; Michael Geist, *Why the USMCA Will Enhance Online Free Speech in Canada*, POLICY OPINIONS (Oct. 4, 2018), https://policyoptions.irpp.org/magazines/october-2018/why-the-usmca-will-enhance-online-free-speech-in-canada/ [hereinafter Geist, *Why USMCA Will Enhance Online Free Speech*]; Michael Geist, *Canada's Missing Internet Provision: Why NAFTA Offers the Chance to Establish Long Overdue Online Speech Safeguards,* MICHAEL GEIST (Dec. 1, 2017), https://www.michaelgeist.ca/2017/12/nafta onlinespeechsafeguard/ [hereinafter Geist, *Canada's Missing Internet Provision*]. Geist argued specifically that "the absence of safe harbour protections has created a disincentive for both new and established services to use Canada to store data or maintain a local presence." Geist, *Why USMCA Will Enhance Online Free Speech, supra* note 144.

145. Goldman, *supra* note 74.

146. USMCA, *supra* note 2, art. 19.17.2, n.7. Arguably, this footnote may qualify not only Article 19.17.2 but also the entire Article 19.17, as it states "a Party may comply with *this Article* through its laws, regulations, or application of existing legal doctrines as applied through judicial decisions." (emphasis added).

147. Geist, *Why USMCA Will Enhance Online Free Speech, supra* note 144.

Canada, defamation has strict liability, so intent is irrelevant.[148] This approach means the law becomes more problematic when applied to intermediaries who play a "peripheral role" in disseminating defamatory information generated by third parties.[149] In *Baglow v. Smith*, for instance, an online forum company was sued for a third-party defamatory statement.[150] Although this company defended itself as playing only a "passive role," the court rejected this view and held that it could be liable because it had been notified of the content and elected not to act.[151]

Applying common law to online intermediaries by treating them as a "publisher" has been featured in the recent reform agenda.[152] The Law Commission of Ontario (LCO), for example, opined that the traditional approach is ill-suited to deal with social media and thus called for statutory reform.[153] Yet, the recommendations reject the CDA 230-type statute because it insufficiently addresses reputational harm arising from online defamation.[154] Instead, the recommendations suggest a model where intermediary platforms who receive a complaint of allegedly defamatory content are required to either notify the content's

148. *See, e.g.*, Hilary Young, *The Canadian Defamation Action: An Empirical Study*, 95-3 CANADIAN BAR REV. 591, 593 (2017); Raymond E. Brown, Defamation Law: A Primer 29 (2nd ed. 2013).

149. LAW COMMISSION OF ONTARIO, DEFAMATION LAW IN THE INTERNET AGE: CONSULTATION PAPER 46 (Nov. 2017).

150. Baglow v. Smith, 2015 O.N.S.C 1175 (Can. Ont. Sup. Ct.).

151. *Id.* at 180–196. Two issues are noteworthy. First, that neither the user nor the forum administrators ultimately were found liable because although the post was *prima facie* defamatory, the "fair comment" defense was made out. Second, it is crucial to clarify the notion of "intermediaries" that are potentially liable for defamation. In Canadian common law, there are two distinct relevant legal doctrines. The first concerns "secondary publishers", the second, "publishers by omission". Secondary publishers are publishers from the outset—they publish the content without knowledge of its defamatory contents (*i.e.,* through negligence). It is different from "publishers by omission"—those that only become responsible after their failure to remove defamatory content. Thus, a secondary publisher only has constructive knowledge, while a publisher by omission has actual knowledge. More precisely, therefore, in *Baglow*, the forum administrators were (prima facie) liable for defamation because they were a "publisher by omission", not a secondary publisher, for they were notified of the defamatory content but failed to remove it. For either "secondary publishers" or "publishers by omission," however, one can see the legal risks of imposing common law duties on online platforms and their potential tension with USMCA Article 19.17. *See* Emily B. Laidlaw & Hilary Young, *Internet Intermediary Liability in Defamation*, 56 OSGOODE HALL L.J. 112, 118–19 (2018) [hereinafter Laidlaw & Young] .

152. *See generally* LAW COMMISSION OF ONTARIO, DEFAMATION LAW IN THE INTERNET AGE: FINAL REPORT, *supra* note 142.

153. Notably, however, in the LCO's view, "the best way for defamation law to continue to develop in a flexible and principled manner is through evolution of the common law," and therefore, it is against "codifying the law in a comprehensive statute." *Id.* at 10.

154. *Id.* at 84.

publisher or take down the content if it is not possible to notify the publisher or if the publisher does not respond.[155] The LCO also recommends that notice and takedown obligations be enforced by a provision for statutory damages; when an intermediary platform fails to comply with notice and/or takedown, a complainant would have the option of seeking a court award in the form of statutory damages against the platform.[156] More crucially, the LCO recommends that the notion "publisher" be narrowed to preclude intermediary liability—that is, "publisher" should refer only to the individual posting the content (the primary publisher), rather than the intermediary hosting it.[157]

It remains to be seen how Canada would reconcile the common law defamatory liabilities and the Intermediary Immunity clause through legislative reform. However, reducing the civil liabilities of online platforms appears in line with Canada's reform agenda, which can provide a level playing field vis-à-vis its United States counterpart and encourage high-tech firms to relocate to Canada. This may well explain why Canada did not further qualify its obligations under USMCA Article 19.17. Additionally, while it is not clear which regulatory model Canada will pursue to reshape defamation liabilities, the textual difference between CDA 230 and USMCA 19.17.2 as noted above suggests that USMCA excludes only "civil liabilities," not equitable relief.[158] Equitable remedies like injunctions would continue to apply.[159] In this light, even though we could read the USMCA as changing the common law liabilities for defamation, the scope of protection is not as sweeping as what we see in the CDA 230 context.

155. *Id.* at 85 (noting that this would apply to "social networks (Facebook, Twitter), media sharing platforms (YouTube), publishing services (Blogger) and other services having a direct hosting relationship with users.").

156. *Id.* at 88.

157. *Id.* at 10, 77–78. Also, the LCO recommends that a publisher should be "defined to require an intentional act of communicating a specific expression." *Id.* at 80.

158. Krishnamurthy & Fjeld, *CDA 230 Goes North American*, *supra* note 6, at 6–9 (observing that CDA 230 (c) bars "all causes of actions," including imposing liabilities and granting equitable relief, while U.S.M.C.A Article 19.17.2 "leaves open the possibility of equitable remedies.").

159. Hugh Stephens further argued that "while the Parties have agreed under the USMCA to not treat a platform as the creator of content, in other words as a primary publisher, platforms are still liable under the Canadian common law as secondary publishers when they knowingly publish the contents of a primary publisher that is, for example, defamatory." Hugh Stephens, *Did Canada Get "Section 230" Shoved Down Its Throats in the USMCA?*, HUGH STEPHENS BLOG (Feb. 10, 2019), https://hughstephensblog.net/2019/02/10/did-canada-get-section-230-shoved-down-its-throat-in-the-usmca/. However, this view may be debatable, for it conflated two concepts—"secondary publisher" and "publisher by omission"—as noted above. *See* Laidlaw & Young, *supra* note 151, at 118–19.

Mexico sits somewhere in the middle. Although Mexico, unlike Canada, maintained carve-outs by Annex 19-A, their effect is not as straightforward as seen in Japan's Side Letter.[160] Notably, Annex 19-A provides Mexico a three-year grace period, which is unavailable for Japan and Canada.[161] Also, Mexico currently has no CDA 230 equivalent, but it remains to be seen how it gives effect to this Immunity Clause, as it has a transition period of three years under Annex 19-A (1).[162] Mexico may continue to address civil liabilities of defamation through, among others, the Federal Civil Code, especially Section 1916 and 1916 *bis*.[163] The issue then is how the Intermediary Immunity clause would affect the operation of the existing law and, more importantly, the policy space to enact new laws.[164] For instance, in 2019, there was a proposal to amend the Federal Civil Code Section 1916 to include social media firms' civil liabilities,[165] which may cast doubt on whether Mexico will make a similar attempt under the USMCA going forward.

160. As noted earlier, the Japan-U.S. Side Letter essentially canceled much of the effect of the Immunity Clause, given the difference between this CDA 230-like provision and the existing Japanese law. *See Japan*-U.S. Side Letter, *supra* note 35.

161. USMCA, *supra* note 2, Annex 19-A.1 (noting Article 19.17 shall not apply to Mexico until three years after USMCA enters into force).

162. *Id.*

163. Juan Carlos Arjona Estévez, *Freedom of Expression in Mexico: Back and Forth,* UNIVERSIDAD DE PALERMO 8–9 (2018), https://www.palermo.edu/cele/libertad-de-expresion/pdf/Freedom_of_expression_in_Mexico.pdf. Mexico's Federal Civil Code Article 1916 addressed moral damage as an injury or harm a person suffers in feelings, dignity, honor, reputation, private life, or public perception. Besides economic indemnification, the court may order the liable person to publish an extract of the final resolution declaring the existence of the moral damage.

164. Article 133 of Mexican Constitution requires judges of each state to observe the Constitution, the laws derived from it and the treaties, "despite any contradictory provision that may appear in the constitutions or laws of the states." It is not clear if one can read into Article 133 of Mexico's Constitution as requiring judges to interpret Sections 1916 and 1916*bis* as narrowly to exclude the civil liabilities of online platforms if we consider both USMCA Article 19.17 and Annex 19-A holistically. *See* Constitución Política de los Estados Unidos Mexicanos, CP, Diario Oficial de la Federación [DOF] 05-02-1917, últimas reformas DOF 17-05-2021 [hereinafter *CP*], art. 133. *See also* Goldman, *Good News*, *supra* note 74 ("Creating a new statutory Internet immunity is a major commitment on Mexico's part, and a very welcome one. The legislative change could spur innovative new Mexican-grown startups as well as open up Mexico to more relocation and job creation by non-Mexican Internet companies.").

165. Report of the Initiatives Presented by the Deputy Nayely Salvador Bojalil within the LXIV Parliament Session Sent to a Commission for its Analysis, Identified as #21 (Iniciativas presentadas por Diputado en la LCIV Legislativa turnadas a Comisión, May 2021) http://sitl.diputados.gob.mx/LXIV_leg/curricula.php?dipt=218. The proposed amendment mentioned, among others, that if the wrongdoer cannot be identified, a social media firm has to remove the content, otherwise it will be liable for the wrongdoing and the relevant non-pecuniary damage.

Central to this question is Annex 19-A, which includes a reference that Mexico will only comply with USMCA Article 19.17.3 in a way that is "both effective and consistent with Mexico's Constitution . . . specifically Articles 6 and 7."[166] These two provisions are the cornerstones for freedom of expression. Mexican Constitution Article 6.1 balances freedom of expression and other public interests by providing: "Expression of ideas shall not be subject to judicial or administrative inquiry, except for those cases when such expression of ideas goes against the moral, privacy or the rights of third parties, causes perpetration of a felony, or disturbs the public order."[167] Articles 6.2 and 6.3 confirm the right to information and underscore the means to achieve it, respectively: "[e]very person shall have free access to public information. . .without the need to prove interest or justification" and "[t]he mechanisms of access to information and quick review procedures shall be established."[168] Mexican Constitution Article 7 reaffirms freedom of expression by clarifying that:

> Freedom of speech, opinion, ideas and information through any means shall not be abridged. Said right shall neither be abridged through any indirect means, such as abuse of official

166. USMCA, *supra* note 2, Annex 19-A.3. Annex 19-A also contains a reference that "The Parties understand that Articles 145 and 146 of Mexico's *Ley Federal de Telecomunicaciones y Radiodifusión*, as in force on the date of entry into force of this Agreement, are not inconsistent with Article 19.17.3 (Interactive Computer Services). In a dispute with respect to this article, subordinate measures adopted or maintained under the authority of and consistent with Articles 145 and 146 of Mexico's *Ley Federal de Telecomunicaciones y Radiodifusión* [Federal Telecommunication and Broadcasting Law (FTBL)] shall be presumed to be not inconsistent with Article 19.17.3 (Interactive Computer Services)." This Law was enacted in 1995 and enabled the private sector to participate in the telecom market so as to develop the nation's telecom infrastructure as its primary driver. It is not thus specifically concerning online platform and its liabilities. Articles 145 and 146 of FTBL establish principles for Internet providers ("the concessionaires") to follow and require them to ensure the quality, capacity, and velocity to their users. However, they apply primarily to the entities that are subject to licenses—online platforms will not fall within unless they use the regulated spectrum. Senator Monreal admitted that online platforms need no permit to operate and are not subject to the existing FTBL. This is also the reason underlying his proposal to regulate them. See Araceli Hernández Zamora, *IFT Sería el Órgano Regulador de Redes: Ricardo Monreal, Asi La Cosas* (Feb. 2, 2021), https://wradio.com.mx/programa/2021/02/02/asi_las_cosas/1612280792_989161.html. In a separate yet related context, the current Mexican President López Obrador has on several occasions attacked social media for censorship that can raise concerns over freedom of speech. *Mexican President Defends Freedom of Speech in Response to Social Media Bill*, REUTERS (Feb. 11, 2021), https://www.reuters.com/article/mexico-socialmedia-idUSL1N2KG22T.

167. CP., *supra* note 164, art. 6.

168. *Id.* art. 6.2–6.3.

> or private control over paper, radio electric frequencies or any other materials or devices used to deliver information, or through any other means or information and communication technologies aimed at impeding transmission or circulation of ideas and opinions.[169]

Two competing views arise. These two provisions, if read broadly, could arguably enable Mexico to adopt measures to hold social media firms liable for civil liabilities. However, an immediate question is: why did Mexico include a three-year grace period in the first place if there is such a useful tool to hold social media companies civilly liable? Amid the ambiguity, Senator Ricardo Monreal launched an initiative in early 2021 to amend the Federal Telecommunications and Broadcasting Law (FTBL) to regulate social media.[170] Citing the concern for freedom of speech,[171] Senator Monreal recommended giving the regulator oversight power to ensure social media firms create an internal complaints procedure for content and suspension or elimination of accounts.[172] Notably, Monreal's initiative would apply only to those social media firms with one million or more users, as they are "capable of generating a greater impact on the process of social communication and legal sphere of citizens."[173] It is not clear whether the final bill, if passed, would also address civil liability issues,[174] although tech firms have already challenged its compatibility with Mexico's commitments under

169. *Id.* art. 7.

170. Senador Dr. Ricardo Monreal Ávila, Initiative, LXIV Legislatura (2021) https://ricardomonrealavila.com/wp-content/uploads/2021/02/REDES-SOCIALES-Propuesta-Iniciativa-29.01.21.pdf [hereinafter *Monreal Initiative*].

171. Ricardo referred specifically to the fact that Article 7 of the Constitution protects the freedom to disseminate opinions, information and ideas. *Id.* at 21.

172. *Id.* at 33, 39 (identifying this proposed amendment as the new article 175 *bis* of the FTBL).

173. *Id.* at 34, 37 (identifying the proposed amendment as the new article 3.LXII of the FTBL).

174. While the civil liability of the online platforms remains unclear, what has been released so far indicates that online platforms would be subject to the regulatory supervision (*i.e.,* Federal Telecommunications Institute—Instituto Federal de Telecomunicaciones (IFT)) and judicial review in relation to content moderation. The initiative seeks to subject social media firms meeting the requirement to license, require them to have clear rules for removing contents, canceling or suspending user accounts, to comply with Constitution Articles 6 and 7, and allow the users to bring the relevant complaints before the regulator (as a first instance) and to initiate a constitutional claim (in case the first one is rejected). *See id.* at 43 (identifying the proposed amendment as the new article 175 Sexies of the FTBL.) *See also* Araceli Hernández Zamora, *IFT Sería el Órgano Regulador de Redes: Ricardo Monreal*, WRADIO (Feb. 2, 2021), https://wradio.com.mx/programa/2021/02/02/asi_las_cosas/1612280792_989161.html.

USMCA Article 19.17.[175] While it is too early to predict how Mexico will reconcile public interest in social media with its treaty obligation, at least some of these criticisms may go too far.[176] For instance, USMCA Article 19.17 immunizes only "civil liability" and should not be interpreted as loosely as depriving Mexico's regulatory power over online platforms from the public law perspective.[177] Even for civil liabilities, we should bear in mind the potentially significant role of Articles 6 and 7 of the Mexican Constitution, as they are embedded in Annex 19-A.

III. The Case Against Intermediary Immunity Clause through Trade

One immediate issue follows from the above: how serious was the U.S. in exporting CDA 230 through trade negotiations? The U.S. could have reduced the carve-outs as much as possible; it does not make sense, at least, to allow Japan to essentially cancel the effect of the Intermediary Immunity clause or Mexico to condition compliance upon its Constitution with a high level of abstraction and dynamism if the U.S. policymakers were keen to make this a new global norm. This question leads to two interrelated claims.

First, the motivation behind the new clause may not be about making CDA a new global norm through trade. Instead, it can be seen as a way of offering a shield against domestic preference changes. By baking

175. Margaret Spiegelman, *Mexican Proposal to Regulate Social Media Companies Sparks USMCA Concerns*, Inside U.S. Trade, Feb. 26, 2021. Not only tech firms, but some civil society groups raised concerns about the compatibility of Moreal's recommendations with the Constitution in relation to freedom of speech and access to information. *See, e.g.*, *#InternetBajoAtaque:la regulación de las redes sociales como mecanismo de control*, Articulo 19, Feb. 5, 2021, at 5, https://articulo19.org/wp-content/uploads/2021/02/Article19_2021-PosicionamientoInternet_v3.pdf.

176. Asociación Latinoaméricana de Internet (ALAI), an industry group including Facebook and Twitter as its members, voiced that the proposal would violate USMCA's provisions on national treatment by requiring special licensing only for certain social networks, erecting unjustified trade barriers to digital trade, and inhibiting cross-border data flow. *See Spiegelman, supra* note 175.

177. USMCA, *supra* note 2, art. 19.17.4. In exercising such power, indeed, Mexico needs to follow the major disciplines such non-discriminatory principle, as per USMCA Annex 19-A.4. Likewise, the Senator also engaged Articles 6 and 7 of Mexico's Constitution arguing that the proposal is consistent with the USMCA obligations. *See* Monreal Initiative, *supra* note 170, at 29 (arguing that this initiative also intends to be consistent with the part of the Annex 19-A, relating to complying with the obligations of Article 19.17.3 in a manner that is both effective and consistent with Mexico's Constitution, specifically Articles 6 and 7 which protect the human right to freedom of expression.). Thus, the civil penalty as included in the proposal as applied to certain social media for breach of the law would not be inconsistent with the USMCA commitments. The maximum fine, as proposed, is up to 1,000,000.00 UMAs (equivalent to 4.4 million dollars approximately). *See* Monreal Initiative, *supra* note 170, at 45 (identifying this proposed amendment as the new article 311 *bis* of the FTBL).

CDA 230 into trade agreements, the U.S. has committed itself to CDA 230, making it difficult to overhaul this controversial legislation at home. For the U.S., the extent to which its trading partners accept this new arrangement seems a secondary concern that turns on bargaining dynamics. The level of sensitivity and the complicated interests underlying this clause is clear to the U.S.—otherwise, the U.S. could have called this clause "safe harbor," as it has done for copyright infringement.

Second, and relatedly, it is because of such complexity and the growing concerns over social media that major trading powers with their regulatory approaches, like E.U. and China, would be less likely to follow the U.S. model. Together, it seems difficult—and in my view, undesirable—to further diffuse this new clause via other trade agreements, as argued below.

A. *Locking the U.S. in with Moderator's Dilemma*

The Intermediary Immunity clause is not as powerful as it appears, at least in the case of Japan and, to a lesser extent, Mexico. Although this new clause may affect Canada, it would surely be binding on the U.S. itself, too. It is common to see international agreements—including international trade and investment treaties—create commitments at the domestic level.[178] Indeed, it is not the first time the U.S. has "locked in rules already on the book" through trade agreements. The U.S. tied its hands, as Professor Kathleen Claussen remarks, with the North American Free Trade Agreement (NAFTA) to recognize Canadian whisky as a distinctive Canadian product and tequila as a distinctive Mexican product—although both were already covered in the existing regimes.[179] The new NAFTA—USMCA repeated the same commitments.[180] CDA 230 is just yet another example creating a lock-in effect, entrenching the status quo.

In fact, the normative implications of the U.S. incorporating CDA 230 in trade agreements have been raised and debated among Republicans, Democrats, and the high-tech industry during the USMCA and Japan-U.S. DTA negotiations. Republican politicians against CDA 230 often claim this law allows tech firms to selectively

178. Tom Ginsburg, *Locking in Democracy: Constitutions, Commitment, and International Law*, 38 N.Y.U. J. INT'L L. & POL. 707, 712 (2006) (arguing that constitutions have been used to lock in democratic norms by incorporating international law principles to strengthen the constitutional pre-commitment to democracy); *see also* Kathleen Claussen, *Regulating Foreign Commerce Through Multiple Pathways*, 130 YALE L.J. FORUM 266 (2020).

179. Claussen, *supra* note 178, at 272.

180. *Id.* at 272–73.

censor and limit their reach on social media and have called for taking CDA 230 language out of trade agreements; Senator Ted Cruz (R-TX), for instance, suggested explicitly that "American trade deals should reflect settled American law, values, and customs. They should not contain provisions that are the subject of ongoing debate."[181] For Cruz, these big tech firms "have become some of the most powerful censors the world has ever seen,"[182] and therefore, social media like Facebook should be "neutral public forums" to be eligible for CDA 230 protection—otherwise, they should be treated as a "'publisher or speaker' of user content if they pick and choose what gets published or spoken."[183] Cruz urged the U.S Trade Representative to remove the text mirroring CDA 230 from USMCA and Japan-U.S. DTA; for him, it would be a "mistake" to enshrine such clauses in the trade agreements, and the two Houses should seriously consider "whether to amend or eliminate Section 230's grant of immunity because Big Tech is not living up to its end of the legislative bargain."[184]

Not only do the Republicans want to abolish CDA 230-type clause: House Speaker Nancy Pelosi (D-CA) also dubbed this as "a gift to big tech companies" and one that could be taken away.[185] There are concerns, according to Pelosi's spokesperson, "about enshrining the increasingly controversial Section 230 liability shield in our trade agreements, particularly at a time when Congress is considering whether changes need to be made in U.S. law."[186] Frank Pallone (D-N.J.), Chairman of the House of Representatives Committee on Energy and Commerce, along with Greg Walden (R-OR), likewise warned that it is "inappropriate" for the U.S. to "export language mirroring Section 230 while such serious policy discussions are ongoing . . . [W]e do not

181. Letter from Ted Cruz, Sen., to Ambassador Robert Lighthizer, U.S. Trade Rep. (Nov. 1, 2019) [hereinafter *Cruz's Letter to Lighthizer*].

182. *Id.*

183. Press Release, Ted Cruz, Senate, Sen. Cruz Op-Ed on FoxNews.com: 'Facebook Has Been Censoring or Suppressing Conservative Speech for Years' (Apr. 11, 2018), https://www.cruz.senate.gov/?p=press_release&id=3718.

184. *Cruz's Letter to Lighthizer*, *supra* note 181, at 1.

185. Eric Johnson, *Silicon Valley's Self-Regulating Days "Probably Should Be" Over, Nancy Pelosi Says*, VOX, (Apr. 12, 2019, 6:20 PM), https://www.vox.com/podcasts/2019/4/11/18306834/nancy-pelosi-speaker-house-tech-regulation-antitrust-230-immunity-kara-swisher-decode-podcast (commenting that "I don't think they are treating it with the respect that they should. . . And so I think that could be a question mark and in jeopardy. . . For the privilege of 230, there has to be a bigger sense of responsibility on it, and it is not out of the question that that could be removed.").

186. Lauren Feiner, *Pelosi Pushes to Keep Tech's Legal Shield Out of Trade Agreement with Mexico and Canada*, CNBC (Dec. 5, 2019, 11:01 AM), https://www.cnbc.com/2019/12/05/pelosi-pushes-to-keep-section-230-out-of-usmca-trade-agreement.html.

believe any provision regarding intermediary liability protections of the type created by Article 19.17 are ripe for inclusion in any trade deal going forward."[187]

On the other hand, tech companies have lobbied strongly to include the immunity language in trade pacts, suggesting that including this shield is needed to give legal certainty for American firms to operate overseas.[188] For instance, Katherine Oyama, global head of Intellectual Property Rights (IPR) policy at Google, explained that nothing in the trade deals would bind Congress' hands.[189] Others commented along the same line in favor of exporting CDA 230 via trade agreements.[190]

Notwithstanding Senators' and Representatives' concerns about lock-in effects,[191] this heavy lobbying by Silicon Valley succeeded in including CDA 230 language in the USMCA and Japan-U.S. DTA.[192] Commenting on this, Speaker Pelosi regretted that she was too late to

187. Letter from Frank Pallone, Jr. & Greg Walden, Chairman & Ranking Member, House Comm. on Energy and Com.,, to Ambassador Robert E. Lighthizer, U.S. Trade Rep. (Aug. 6, 2019).

188. John D. McKinnon & Brody Mullins, *Nancy Pelosi Pushes to Remove Legal Protections for Online Content in Trade Pact*, WALL ST. J. (Dec. 4, 2019, 6:45 PM), https://www.wsj.com/articles/nancy-pelosi-pushes-to-remove-legal-protections-for-online-content-in-trade-pact-11575503157.

189. Feiner, *supra* note 186.

190. *See, e.g.*, Michael Petricone, *Protect Online Free Speech: Keep Section 230 Language in USMCA*, CONSUMER TECH. ASS'N, (Dec. 5, 2019), https://www.cta.tech/Resources/Newsroom/Media-Releases/2019/December/Protect-Online-Free-Speech-Keep-Section-230-Langua (arguing that inclusion of CDA 230 in trade agreements does not stop the US from changing the law in the future should it choose to do so). The Software Alliance, an industry group that counts Apple, Microsoft and Intel among its members also contended that "U.S. exporters and well-paid American coding and programming jobs depend on having legal certainty abroad regarding liability. Having a principle enshrined, that those companies will not be held liable for content over which they have no direct control, is useful and important." See Dean DeChiao, '*A Real Gift to Big Tech': Both Parties Object to Immunity Provision in USMCA*, ROLL CALL, (Dec. 17, 2019, 7:00 AM), https://www.rollcall.com/2019/12/17/a-real-gift-to-big-tech-both-parties-object-to-immunity-provision-in-usmca.

191. Gretchen Peters, Executive Director of the Alliance to Counter Crime Online, also added that exporting CDA 230 via trade deals is "problematic because it potentially is going to tie Congress' hands from reforming the bill down the line, and that's precisely why industry is pushing to have it inside the trade deals." Feiner, *supra* note 186.

192. USMCA was approved under the Trade Promotion Authority (TPA)—often known as the "fast-track" process authorized by the Bipartisan Congressional Trade Priorities and Accountability Act of 2015. Thus, Congress has its final say in the form of an up-or-down vote on the implementing bill of the USMCA—The United States-Mexico-Canada Agreement Implementation Act —approved by the House in December 2019 by a vote of 385-41 and by the Senate in January 2020 by a vote of 89-10. By contrast, Japan-U.S. DTA was considered an executive agreement and no formal action from Congress was needed. *See* CONG. RSCH. SERV., IF10997, U.S.-MEXICO-CANADA (USMCA) TRADE AGREEMENT (2021); CONG. RSCH. SERV., IF11120, U.S.-JAPAN TRADE AGREEMENT NEGOTIATIONS (2020).

address it: "I lost — they had 230 in the agreement, there are some members that wanted that . . . it's a real gift to big tech."[193] These negotiation dynamics provide valuable insights.

First, if the legal risks in overseas markets are of concern to Silicon Valley, the Intermediary Immunity clause can provide them better protection in Canada—but this is much less obvious in the case of Mexico and Japan. The real gain of baking CDA 230 into trade agreements would be entrenching the status quo of CDA 230 at home, while attempting to diffuse this regime as a new global norm.[194]

Over the years, CDA 230 has been the host of controversies as a matter of law, policies, and politics. The back-and-forth debate around the role of CDA 230 and the broad immunity afforded to online intermediaries for content-hosting and moderation decisions is nothing new. The debate escalated when President Trump, apparently responding to the treatment of his posts by social media giants, issued Executive Order 13925 in May 2020, titled "Preventing Online Censorship."[195] The Department of Justice (DOJ) followed with a review in June 2020 that mapped key issues of reform, like removing protections from civil lawsuits brought by the federal government and clarifying the purpose of the section via amended definitions to "good faith."[196] In July 2020, the Commerce Department, as this Executive Order directed, filed a rulemaking petition before the Federal Communications Commission (FCC) to clarify CDA 230 to bring greater transparency regarding how online platforms moderate their websites.[197]

193. Chris Mills Rodrigo, *Tech Legal Shield Included in USMCA Despite Late Pelosi Push,* THE HILL (Dec. 10, 2019, 1:45 PM), https://thehill.com/policy/technology/473905-tech-legal-shield-included-in-usmca-despite-late-pelosi-push?rl=1. In the public hearing dedicated to digital trade, there were discussions on digital trade in general and some specifically related to data protection, though CDA 230 was not singled out. *The Need for U.S. Leadership on Digital Trade: Hearing Before the Joint Econ. Comm.*, 115th Cong. (2018).

194. It remains to be seen, however, whether the US could successfully replicate the Intermediary Immunity clause in other trade deals down the path—and the extent to which its trading partners could push by with qualifications on it. This would determine the contour of the CDA 230 emerging as a new global norm. *See* discussion *infra* Section III.2.

195. Exec. Order No. 13,925, 85 Fed. Reg. 34,079 (June 2, 2020).

196. U.S. Dep't of Just., Key Takeaways and Recommendations: Section 230—Nurturing Innovation or Fostering Unaccountability? (2020), https://www.justice.gov/file/1286331/download.

197. David Shepardson et al., *Trump Administration Petitions FCC on Social Media Content Rules, Reuters* (July 27, 2020, 6:37 PM), https://www.reuters.com/article/us-twitter-trump-idUSKCN24S2QM.

Since 2020, there have been more than twenty bills before Congress for CDA 230 reform.[198] Of those, twenty are currently live in the 117th Congress.[199] Some of these proposals are noteworthy. The "Online Freedom and Viewpoint Diversity Act" and "Limiting Section 230 Immunity to Good Samaritans Act" have been proposed by Republican lawmakers to narrow CDA 230's immunity; the former offers the immunity only to online intermediaries with an "objectively reasonable belief" that content falls within a specific category before they restrict access to it,[200] and the latter prevents them from being protected unless they update their terms of service relating to any policies on restricting access to or availability of the material in good faith.[201] Democrats likewise proposed the "Safeguarding Against Fraud, Exploitation, Threats, Extremism and Consumer Harms (SAFE TECH) Act" that scales back the scope of the immunity in two crucial ways.[202] First, the bill proposes to make CDA 230 immunity apply only to "speech" posted by another person and not broadly "information."[203] Second, this bill would pierce the legal shield of online intermediaries who have "accepted payment to make the speech available or, in whole or in part, created or funded the creation of the speech."[204] The "Platform Accountability and Consumer Transparency (PACT) Act," a bipartisan bill, seeks to strengthen online transparency, accountability, and consumer protection by requiring online platforms to have "acceptable use policy" that informs users of their content moderation policy upfront and maintain a procedure for users to make complaints.[205]

198. Megan Anand et al., *All the Ways Congress Wants to Change Section 230*, SLATE (Mar. 23, 2021, 5:45 AM), https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html (providing a comprehensive list).

199. *Id.* A few more have been proposed since Anand's survey. *See* Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong. (2021) (introduced Mar. 23, 2021, and referred to the Communications and Technology Subcommittee of the House Committee on Energy and Commerce); 21st Century FREE Speech Act, S. 1384, 117th Cong. (2021) (referred to the Senate Committee on Commerce, Science, and Transportation); Civil Rights Modernization Act of 2021, H.R. 3184, 117th Cong. (2021) (introduced May 13, 2021, and referred to the House Committee on Energy and Commerce); SAFE TECH Act, H.R. 3421, 117th Cong. (2021) (introduced May 20, 2021, and referred to the House Committee on Energy and Commerce).

200. Online Freedom and Viewpoint Diversity Act, S. 4534, 116th Cong. § 2 (2020).

201. Limiting Section 230 Immunity to Good Samaritans Act, S. 3983, 116th Cong. § 2 (2020).

202. SAFE TECH Act, S. 299, 117th Cong. § 2 (2021).

203. *Id.*

204. *Id.*

205. Platform Accountability and Consumer Transparency Act, S. 4066, 116th Cong. § 5 (2020).

These various proposals reflect the growing concern of both parties in relation to the role of CDA 230—albeit based on different rationales. For Republicans, the proposals reflect conservatives' belief that tech platforms restrict or censor conservative opinions, exemplified by the banning of President Trump from Twitter on January 8, 2021.[206] Democrats, meanwhile, push the reform to not only curb harmful illegal activity but also to make social media "less hostile towards speech from marginalized groups struggling for social, economic and racial justice."[207]

President Biden in mid-May 2021 revoked Executive Order 13925 by former President Trump.[208] In doing so, President Biden essentially offered a clean slate for both parties and the White House to discuss reforms anew.[209] Even though there seems to be an appetite for CDA 230 reform and some consensus on the need to re-examine the CDA in light of the new digital age, the parties diverge greatly on the reasons

206. Jessica Guynn, *Donald Trump and Rudy Giuliani Blast Facebook, Twitter over Alleged Censorship and Bias for Joe Biden: 'It's a fix'*, USA TODAY (Nov. 3, 2020, 6:21 PM), https://www.usatoday.com/story/tech/2020/11/03/facebook-twitter-trump-giuliani-censorship-bias-biden-election-2020/6149742002/; Marguerite Reardon, *Democrats and Republicans Agree That Section 230 is Flawed*, CNET, (Jun. 21, 2020, 8:00 AM), https://www.cnet.com/news/democrats-and-republicans-agree-that-section-230-is-flawed/; Isobel Asher Hamilton, *Here's What Could Happen to Section 230 – the Internet Law Donald Trump Hates – Now the Democrats Have Both Houses*, BUSINESS INSIDER (Jan. 9, 2021, 9:00 AM), https://www.businessinsider.com.au/future-of-section-230-democrats-both-houses-2021-1?r=US&IR=T.

207. Mark MacCarthy, *Back to the Future for Section 230 Reform*, BROOKINGS, (Mar. 17, 2021), https://www.brookings.edu/blog/techtank/2021/03/17/back-to-the-future-for-section-230-reform/; *see*, Press Release, Mark R. Warner, Sen., Warner, Hirono, Klobuchar Announce the SAFE TECH Act to Reform Section 230 (Feb. 5, 2021), https://www.warner.senate.gov/public/index.cfm/2021/2/warner-hirono-klobuchar-announce-the-safe-tech-act-to-reform-section-230; *Top Democrat Speaks to Biden Staff About Key Internet Law*, REUTERS (Mar. 22, 2021, 1:01 PM), https://www.reuters.com/article/us-usa-democrat-tech-idUSKBN2BE2EG.

208. In an interview with the New York Times in January 2020, Joe Biden said that the problem of Facebook's and other platforms' immunity was so great that "Section 230 should be revoked, immediately should be revoked." *See* The Editorial Board, Opinion, *Joe Biden: Former Vice President of the United States, N.Y. Times* (Jan. 17, 2020), https://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html?smid=nytcore-ios-share; However, now that Biden is in power, prevailing opinion is that wholesale reform is unlikely, with an incremental approach apparently preferred by Biden, for complexity of the political divides over this issue. Exec. Order No. 14,029, 86 Fed. Reg. 27,025 (May 14, 2021); Rachel Lerman, *Social Media Liability Law is Likely to Be Reviewed under Biden*, Wash. Post (Jan. 19, 2021), https://www.washingtonpost.com/politics/2021/01/18/biden-section-230/; Jeffrey D. Neuburger, *The President Revokes Prior Administration's Executive Order on CDA Section 230*, *Nat'l L. Rev.* (May 17, 2021), , https://www.natlawreview.com/article/president-revokes-prior-administration-s-executive-order-cda-section-230.

209. Neuburger, *supra* note 208. *See Top Democrat Speaks to Biden Staff About Key Internet Law*, REUTERS (Mar. 22, 2021, 1:01 PM), https://www.reuters.com/article/us-usa-democrat-tech-idUSKBN2BE2EG.

and focus of such reforms, making any potential initiative likely to be incremental under the Biden Administration, rather than a wholesale rewrite.[210] The U.S. under Trump Administration appeared to have acted inconsistently by adding a CDA 230-type arrangement—something Republicans vowed to review and reform—in recent negotiations with Kenya and the U.K.,[211] as well as the WTO 2020 E-Commerce Negotiation Text.[212]

President Biden would be wise to reverse the trend by dropping CDA 230 text in trade agreements going forward if there is a serious plan for CDA 230 reform. Otherwise, such language would further undermine the credibility of the U.S. to live up to its commitments, causing problems when working with its trading partners on digital trade issues going forward.[213] Regardless of the growing interest in overhauling CDA 230, the high-tech industry has successfully impeded efforts to modify this legislation domestically significantly.[214] At the very least, passing something like the SAFE TECH Act would be difficult without first considering its implications for international trade commitments. The political complexity of CDA 230 in the U.S., with the underlying concerns about social media in other jurisdictions, as explained below,

210. Neuburger, *supra* note 208.

211. Nandita Bose, *Democrats Prefer 'Scalpel' Over 'Jackhammer' to Reform Key U.S. Internet Law*, REUTERS (Oct. 29, 2020, 6:10 AM), https://www.reuters.com/article/us-usa-tech-liability/democrats-prefer-scalpel-over-jackhammer-to-reform-key-u-s-internet-law-idUKKBN27E1IA. Counter-intuitively, a report shows that "there is no statistical evidence to support the argument that Facebook does not give conservative views a fair shake" when Republicans claim these social media firms are politically biased. *See* Bobby Allyn, *Facebook Keeps Data Secret, Letting Conservatives Bias Claims Persist*, NPR NEWS, (Oct. 5, 2020, 5:00 AM), https://www.npr.org/2020/10/05/918520692/facebook-keeps-data-secret-letting-conservative-bias-claims-persist. In fact, it is common to see Republicans appear on Facebook's 10 top-performing links. *E.g.*, Facebook's Top 10 (@FacebooksTop10), TWITTER, (May 22, 2021, 8:50 PM), https://twitter.com/FacebooksTop10/status/1396871226841178115?s=20&t=BfeXjI71RNPjP7gelqpdsA (reporting that top-performing links on Facebook are by Sean Hannity, Ben Shapiro, Sean Hannity, LA Times, and Ben Shapiro). The fact that these platforms are crucial outlets for conservatives may explain in part why it could be an idea to entrench the status of CDA 230 through trade pacts and also showcase the complexity around CDA 230—even within conservatives. OFF. OF THE U.S. TRADE REP., UNITED STATES-KENYA NEGOTIATIONS, SUMMARY OF SPECIFIC NEGOTIATING OBJECTIVES, AT 7 (2020); OFF. OF THE U.S. TRADE REP., UNITED STATES-UNITED KINGDOM NEGOTIATIONS, SUMMARY OF SPECIFIC NEGOTIATING OBJECTIVES, AT 6 (2019).

212. WTO 2020 E-Commerce Negotiation Text, *supra* note 15, at 24.

213. Gilad Edelman, *On Section 230, It's Trump vs. Trump*, WIRED, (Dec. 3, 2020, 1:39 PM), https://www.wired.com/story/section-230-repeal-its-trump-vs-trump/ (also arguing that while CDA 230 reform is possible, but this "would be weakening other countries' faith that the US honors its international agreements. . .").

214. *See* Bose, *Democrats Prefer "Scalpel"*, *supra* note 210.

would make it problematic—and undesirable—for the Intermediary Immunity clause to be used as a new template in the future negotiations.

B. *MY Trade, Your First Amendment—External Boundaries of Intermediary Immunity*

The Intermediary Immunity clause only appears in recent U.S.-led trade negotiations; none of other major trading powers like China and E.U. include similar arrangements in their existing trade agreements. Notably, the U.S.'s plan to include online platform liabilities in its negotiations has already set off the alarm for its trading partners. The U.K. is a prime example; whether or not to include a CDA 230-type clause is hotly contested. BSA—the Software Alliance who lobbied strongly for exporting CDA 230 in the U.S. noted above—supported the addition of the Intermediary Immunity clause in the ongoing U.K.-U.S. trade negotiations, urging policymakers to "ensure that internet intermediaries are protected against liability for unlawful content posted or shared by third parties."[215]

Others are strongly against this view, pointing to the difference between the U.S. and U.K. models regulating intermediaries' liabilities and the judgment call underlying them. For example, Carnegie U.K. Trust argued that changing the regime to CDA 230 approach "would be handing an advantage to American companies over U.K. ones and would disadvantage U.K. citizens and consumers who would be entitled to lesser protection."[216] Carnegie U.K. Trust then called on the U.K. government to consider legal certainty and relevant costs against the backdrop of CDA 230 and the First Amendment in the U.S.:

> The U.K. government would of course consider the substantial regulatory uncertainty that would be introduced in switching to a new regime. If the U.K. were to move to an American-style regime there would be uncertainty about the compatibility of statutory duty of care with the First Amendment to the U.S. Constitution as well as a 'statutory' duty of care being a novel instrument in American law. The immediate reaction of a party

215. BSA The Software All., The Software Alliance's Evidence on Digital Trade and Data: Submission to the House of Commons' International Trade Select Committee, ¶ 22 (2021) (U.K.), https://committees.parliament.uk/writtenevidence/22604/pdf/.

216. Carnegie UK Trust, Submission to International Trade Committee Call for Evidence on Digital Trade and Data (2021) (U.K.), https://committees.parliament.uk/writtenevidence/22619/pdf/ [hereinafter *Carnegie Submission*].

> would be to litigate to establish whether a statutory duty can operate at all with a S230 approach and seek to introduce First Amendment issues. Such litigation would take years to conclude, undermining the regime. We note that the largest American companies in this sector have around $200 billion cash at hand and thus long pockets for litigation purposes.[217]

Carnegie Trust U.K. concluded by arguing that: "[l]ocking a version of S230 in a USMCA-like trade deal would ill-serve the U.K."[218] Similar concerns were made by a group of academics from Oxford University, who raised that CDA 230 is "highly contentious" and that policymakers around the world "*are under pressure to clamp down on online harms and the online dissemination of illegal content and many countries—including the U.K., U.S., and E.U.—are currently revisiting their domestic legislation on intermediary liability.*"[219] For this reason, they urged the U.K. government to "carefully consider any interaction between trade policy and domestic regulation of the internet, in particular when it comes to online harms policy," taking into account the "right balance between competing policy goals and establish[ing] a robust domestic regime before signing up to any commitments. . .that could restrict regulatory options."[220] They urged the British policymakers to ensure "commitments in international trade agreements on the liability of online platforms are fully aligned with domestic laws and policies, in particular when it comes to moderation of online content and online harms."[221]

---

217. *Id.* ¶ 14.

218. *Id.* ¶ 18.

219. Emily Jones et al., Submission to the International Trade Committee, UK House of Commons Inquiry on Digital Trade and Data ¶ 38 (2021) (U.K.), https://committees.parliament.uk/writtenevidence/22646/pdf/ (emphasis added) [hereinafter Jones et al, *Submission to the UK ITC*].

220. *Id.* ¶ 40.

221. *Id.* ¶ 41. CDA 230 is different from the British model. Under § 5 of the Defamation Act 2013, for instance, a website operator will not be held liable for hosting defamatory content provided that they properly handle any notices of complaint pertaining to that content. The required procedure is set out in the Regulations. Within 48 hours of an individual submitting a notice of complaint, the website hosting the content must contact the person who posted it (the "poster") or, if they cannot contact that person, remove the content. When contacted in this way, the poster can then respond by either consenting to or refusing to consent to the content's removal. If the poster consents to the removal or fails to respond, the website must remove the content within 48 hours. As long as the website operator acts in accordance with this process–which essentially consists of passing on notices within certain timeframes and/or removing the content when required—then they will be protected from liability. Defamation Act 2013, c. 26 (UK); The Defamation (Operators of Websites) Regulations 2013, SI 2013/3028, regul. 3 and

These are valid concerns. They reflect the challenges facing governments in handling fake news, hate speech, and online defamation while safeguarding the fundamental rights of freedom of expression. Each country has a different regulatory framework that reflects the judgment call of balancing competing interests and does not fit squarely into CDA 230 and the underpinning First Amendment.

The CDA 230 regime as exported via the USMCA and Japan-U.S. DTA is clearly inconsistent with that of the E.U.'s Directive 2000/31/E. C. (E-Commerce Directive) and the Digital Services Act (DSA).[222] While under the E.U. model, online platforms are also protected against liability for third-party content, the conditions are more narrowly crafted; immunity is available to intermediaries operating as "mere conduit,"[223] "caching,"[224] and "hosting" entities and only when their activities are "of a mere technical, automatic and passive nature."[225] Crucially, although the Intermediary Immunity Clause follows CDA 230 by protecting online platforms for taking hands-off or hands-on approach towards third-party content, modifying the information could pierce the legal shield under the E.U. model.[226] Further, the E.U. takes the "notice and takedown" approach by requiring intermediaries (serving, caching, and hosting services) with "actual knowledge" of illegal content to expeditiously to remove or to disable access to it,

sch. (UK). *See* Daithí Mac Síthigh, *The Fragmentation of Intermediary Liability in the UK*, 8(7) J. INTELL. PROP. L. & PRAC. 521, 527–528 (2013).

222. 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, 2000 O.J. (L 178) [hereinafter E-Commerce Directive]; Proposal for a Regulation of The European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM (2020) 825 final [hereinafter Digital Services Act]. The Digital Services Act was passed by the European Parliament on July 5, 2022. It is now pending the formal approval of the Council. Eur. Parliament, *Digital Services: Landmark Rules Adopted for a Safer, Open Online Environment*, https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopeted-for-a-safer-open-online-environment (last visited Aug. 5, 2022).

223. E-Commerce Directive, *supra* note 222, art. 12; Digital Services Act, *supra* note 222, art. 3.

224. E-Commerce Directive, *supra* note 222, art. 13; Digital Services Act, *supra* note 222, art. 4.

225. E-Commerce Directive, *supra* note 222, art. 14; Digital Services Act, *supra* note 222, art. 5.; E-Commerce Directive, *supra* note 222, recital 42.

226. E-Commerce Directive, *supra* note 222, arts. 12–13; Policy Department A: Economic and Scientific Policy, Directorate-General for Internal Policies, Providers Liability: From the eommerce Directive to the Future, Eur. Parl. Doc. (PE 607.349) at 24 [hereinafter Providers Liability]. There was no Good Samaritan clause under the E-Commerce Directive. Article 6 of the proposed DSA however contains such an arrangement. Proposed Digital Services Act, *supra* n.222, art. 6.

otherwise they may lose immunity protection.[227] Online intermediaries' obligations to remove illegal information under threat of liability where they have actual knowledge of the content amounts to "measures that treat a supplier . . . of an interactive computer service as an information content provider"—something forbidden by USMCA Article 19.17.2.[228]

In China, there is no stand-alone legislation like CDA 230; online defamation is governed by the Chinese Civil Code as a matter of tort liability.[229] Built upon the now-revoked Tort Law,[230] the current Chinese model features some sort of notice and takedown flavor requiring online intermediaries to "take necessary measures" upon receiving the notice—along with preliminary evidence of infringement and identity information—from the aggrieved party.[231] Failure to react in a timely manner would make intermediaries "jointly and severally liable" with the users for damages that occurred.[232] Notably, both the Tort Law and the Civil Code can apply to not only online defamation but also copyright infringement, as online intermediaries' tort liabilities are modeled on the DMCA safe harbor in the U.S.[233]

227. E-Commerce Directive, *supra* n.222, arts. 13–14. Notably, E-Commerce Directive applies not only to defamatory statements, but intermediaries who host, cache, or carry other unlawful materials, such as pornography or materials involving IPR infringement. *See* MATTHEW COLLINS, COLLINS ON DEFAMATION 348 (2014).

228. USMCA, *supra* note 2, art. 19.17.2.

229. Zhonghua renmin gongheguo minfa dian (中华人民共和国民法典) [Civil Code of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., May 28, 2020, effective Jan. 1, 2021), arts. 1194–97 [hereinafter PRC Civil Code]. Article 1194 sets out the general principle of online tort liability, followed by a detailed notification process and relevant consequences in Articles 1195 and 1196. Article 1197 establishes the civil liabilities where an intermediary "knows" or "should know" the infringement.

230. Zhonghua renmin gongheguo fading zeren fa (中华人民共和国侵权责任法) [Tort Law of the People's Republic of China], art. 36.

231. PRC Civil Code, *supra* note 229, art. 1195 (1). Article 36 of the Tort Law was criticized for not providing clear instructions as to notice and take down and this has been somewhat fixed by the new Civil Code. Articles 37 and 38 of the Electronic Commerce Law also contain similar provisions concerning online intermediaries' liabilities. *See* Zhonghua renmin gongheguo dianzi shangwu fa (中华人民共和国电子商务法) [Electronic Commerce Law] (effective Jan. 1, 2019).

232. PRC Civil Code, *supra* note 229, art. 1195(2). To be clear, however, online intermediaries shall be liable for "any additional harm" caused to the aggrieved party.

233. *See, e.g.*, Dong Zhu, *Transplantation and Transformation of the ISP's Secondary Liability*, 31 (5) PEKING U.L.J. 1340, 41 (2019) (noting that Article 36 was modelled on the safe harbor under DMCA of the U.S.) Notably, China's Supreme Court in 2014 issued a set of rules explaining how the Civil Code could be applied to online defamation—for instance, factors to establish online intermediaries' knowledge of alleged wrongdoing. Therefore, while the notice and takedown approach was modelled on the DMCA for copyright infringement, the tort liability under the new Civil Code, as it stands today, is broad enough to cover online defamation. Zuigao renmin fayuan guanyu shenli qinhai xinxi wangluo chuanbo quan minshi jiufen anjian shiyong falu ruogan

Other countries frame liability in terms of website operators having "awareness" or "actual knowledge."[234] For example, in Australia, another common law jurisdiction, Schedule 5, Clause 91 of Australia's Broadcasting Services Act 1992 provides that internet content hosts will not be liable for third-party content under state or territory laws if they were "not aware of the nature" of the content.[235] Although the clause has not been subject to significant judicial consideration and there is a degree of uncertainty as to what constitutes "awareness,"[236] one possible interpretation has been suggested: the host loses the benefit of the defense when the existence of the content is drawn to its attention and will accrue liability if it does not act within a reasonable period.[237] In practice, this would not be too dissimilar from the "notice and takedown" model described above. If a content host is notified of defamatory content (thus becoming "aware" of it) and does not act appropriately, they may be held liable as a publisher of that content. Other nations like India and the Philippines also have provisions along these lines.[238]

Clearly, the Intermediary Immunity clause does not necessarily fit into other countries' existing defamation laws. It is problematic for these countries to accept the Intermediary Immunity clause without reconfiguring their regulatory framework unless they put in place qualifications, as in the case of Japan. Underlying the textual differences, more crucially, is how these countries balance freedom of speech and

---

wenti de guiding (最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定) [Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks] (Fa Shi [2020] No. 19, effective Jan. 1, 2021).

234. Ashley Johnson & Daniel Castro, *How Other Countries Have Dealt with Intermediary Liability*, INFO. TECH & INNOVATION FOUND. 1 (Feb. 2021).

235. *Broadcasting Services Act 1992* (Cth), s 5, pt 91(1)(a) (Austl.).

236. Peter Leonard, *Safe Harbors in Choppy Waters - Building a Sensible Approach to Liability of Internet Intermediaries in Australia*, 3 J. INT'L MEDIA & ENT. L. 221, 223, 260 (2010).

237. *Id.* at 260 (quoting the "Defamation" chapter in THE LAW OF ECOMMERCE ¶ 70, 2701 (Adrian Lawrence ed., 2003)); Kylie Pappalardo & Nicolas Suzor, *The Liability of Australian Online Intermediaries*, 40 SYDNEY L. REV. 469, 492 (2018).

238. *See* Information Technology Act, No. 21 § 79, Acts of Parliament, 2000 (India). This provides that an intermediary shall not be liable for third-party content unless "upon receiving actual knowledge . . .the intermediary fails to expeditiously remove or disable access to that material"; *See* An Act Providing for The Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use Thereof, and for Other Purposes, Rep. Act No. 8792, § 30 (June 14, 2000) (Phil.) (short title "Electronic Commerce Act of 2000"). This provides that a service provider shall not be liable for third-party content unless it has "actual knowledge" or is aware that the content is "unlawful or infringes any rights subsisting in or in relation to such material"; Johnson and Castro, *supra* note 234, at 1.

other competing interests. A prime example is the E.U. Its E-Commerce Directive makes clear that it is crucial to strike "a balance between different interests at stake,"[239] and underscores, in particular, the freedom of expression when it comes to content moderation.[240] The E-Commerce Directive hence bars member states from imposing duties on intermediaries to monitor the users' activities;[241] the Court of Justice of the European Union (CJEU) has also confirmed—at least in the context of copyright—that the E.U. law has no space for proactive monitoring and filtering mechanisms.[242]

Yet, in practice, the notice and takedown model often incentivizes platforms to remove more content than necessary.[243] When a platform receives a complaint, the hefty liability that attaches to a failure to take down content that is found to be illegal may outweigh the cost to the platform of over-moderating by removing content that is marginal or not illegal at all. Providers can "reduce false negatives (the distribution of illegal information) by increasing false positives (the removal of legal information)."[244] This has led to concerns over the chilling effect stemming from the current regime.[245] Such concerns are apposite, for private firms may lack the knowledge to assess the legality of content properly. Over-removal is encouraged, thus creating censorship and potential for abuse, without providing the creator of the removed material an opportunity to defend their expression.[246] Therefore, not only freedom of expression but the right to due process is engaged.

In the recitals to the E-Commerce Directive, the E.U. emphasized that safeguards for the fundamental rights were a matter for self-

239. E-Commerce Directive, *supra* note 222, recital 41.

240. *Id.* recital 46.

241. *Id.* art. 15.

242. *See, e.g.*, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, C-360/10 (2012).

243. *See, e.g.*, Johnson & Castro, *supra* note 234; *see also* HOUSE OF LORDS , REGULATING IN A DIGITAL WORLD 47 (2nd Rep. Session 2017-19) (U.K.) (noting that "In practice service providers frequently monitor content, often using specifically designed software, and they work with designated organization. . .to identify illegal content.").

244. Giovanni Sartor, *Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?,* INT'L DATA PRIVACY L. 3, 4 (2012).

245. *See, e.g.,* Aleksandra Kuczerawy, *The Power of Positive Thinking: Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression*, 8 (3) J. INTELL. PROPERTY, INFO. TECH. & E-COM. L. 226 (2017) (arguing that "private entities are co-opted by the State to make decisions affecting the fundamental right to freedom of expression.") [hereinafter Kuczerawy, *Positive Thinking*].

246. Aleksandra Kuczerawy, *Intermediary Liability* & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative, ICRI Working Paper 21/2015, 7 (2015).

regulation by members.[247] However, many members simply implemented the Directive verbatim without applying the additional safeguards, suggesting the rights may be inadequately protected.[248] Commentators concerned with the lack of protection for freedom of expression, therefore, called on the European Court of Human Rights (ECtHR) and CJEU jurisprudence to support their position that the notice and takedown approach is problematic.[249] However, recent jurisprudence seems to suggest the two European courts are re-balancing the competing interests when it comes to intermediary liabilities.

For instance, the CJEU in *Eva Glawischnig-Piesczek v. Facebook Ireland Limited* considered the scope of Art. 15 of the E-Commerce Directive, and clarified that the Directive does not preclude EU member states' national courts from ordering hosting platforms to remove illegal user-generated content, and any content which is "identical" or "equivalent" to content which has previously been declared illegal, on a world-wide basis.[250] While CJEU was careful not to impose a general obligation of human assessment, only requiring automatic systems for moderation,[251] the decision revealed the court's willingness to extend the content moderation to restrict illegal content. Similar views can be seen in ECtHR cases like *Delfi AS v. Estonia*; although it did not discuss the E-Commerce Directive, the decision demonstrates that even the ECtHR is prepared to permit a greater role for content moderation with consequential risk to freedom of expression.[252]

This balancing act becomes more difficult when placed in the context of hate speech and misinformation. The Explanatory Memorandum of the DSA made clear that the proposal aims to "foster responsible and diligent behavior by providers of intermediary services to ensure a safe online environment, which allows . . . to freely exercise

247. *E-Commerce Directive*, *supra* note 222, recital 40.

248. *See, e.g.*, Kuczerawy, *Positive Thinking*, *supra* note 245; Giancarlo F. Frosio, *The Death of 'No Monitoring Obligations' A Story of Untamable Monsters*, 8 (3) J. INTELL. PROP., INFO. TECH. & E-COM. L. 199 (2017).

249. *See, e.g.*, Kuczerawy, *Positive Thinking*, *supra* note 245; ARTICLE 19, *Response to EU Consultation on E-Commerce Directive* (Nov. 2010), https://www.article19.org/data/files/pdfs/submissions/response-to-eu-consultation.pdf.

250. *See* Case C-18/18, Eva Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:821, ¶ 54 (June 4, 2019).

251. *Id.* ¶¶ 46, 53. The CJEU said that for a message to be identical or equivalent, the differences should not be so great as to require "an independent assessment" beyond that which could be conducted by automated technology.

252. Delfi AS v. Estonia, App. No. 64669/09, 09 Eur. Ct. H.R. (2015).

their fundamental rights, in particular the freedom of expression and information."[253] Some proposed changes are noteworthy.

First, the DSA features something similar to the Good Sarmatian protection under CDA 230 which could help eliminate existing disincentives for online platforms to voluntarily investigate their own companies.[254] Moreover, the draft DSA imposes additional obligations to hold online platforms, especially "very large online platforms" (VLOPs) accountable.[255] By targeting VLOPs, the DSA seeks to address misinformation and hate speech issues where they materialize, while not overburdening providers unconcerned by those problems.[256] VLOPs under the new scheme are obliged to conduct risk assessments on systemic risks;[257] take "reasonable and effective measures" to mitigate those risks;[258] and to submit to audits.[259] The DSA underscores, crucially, that risk assessments should consider any negative effect on the freedom of expression and information.[260] All these measures put in place under the DSA are designed to be proportionate to the provider's ability to comply with them.[261]

Even in the shadow of the impending DSA, E.U. member states are divided on how to deal with hate speech and content control. Germany's Network Enforcement Act (NetzDG Law), anti-hate speech legislation, requires online platforms with more than two million users to provide a mechanism for complaints about illegal content and remove unlawful content within 24 hours;[262] failure to do so risks fines

253. Digital Services Act, *supra* note 222, Explanatory Memorandum, at 6.

254. *Id.* art. 6. *See* Aleksandra Kuczerawy, *The Good Samaritan that Wasn't: Voluntary Monitoring under the (Draft) Digital Services Act*, VERFASSUNGSBLOG (Jan. 12, 2021), https://verfassungsblog.de/good-samaritan-dsa/.

255. Digital Services Act, *supra* note 222, art. 25–33.

256. *See, e.g.*, Zohar Efroni, *The Digital Services Act: Risk-Based Regulation of Online Platforms*, INTERNET POLICY REVIEW (Nov. 16, 2021), https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606 (noting that this reveals the risk-based approach and the obligations correspond to the "type and magnitude of the risks online platforms create. . .The bigger an online platform is, the greater is it impact, and hence, the higher are the risks it poses to individuals and society.").

257. Digital Services Act, *supra* note 222, art. 26.

258. *Id.* art. 27.

259. *Id.* art. 28.

260. *Id.* art. 26(1)(b).

261. Digital Services Act, *supra* note 222, Explanatory Memorandum, at 11.

262. Netzwerkdurchsetzungsgesetz [Network Enforcement Act] [NetzDG] art. 1, §§. 1(2), 3(2) 2 (Ger.).

of up to five million euros.[263] The NetzDG Law was attacked for promoting "over-removal" of content, given the short timeframe and the heavy fines available, and for being over-broad in its definition of "unlawful content," for example by including blasphemy.[264] Although there are debates between those fearing a reduction of freedom of speech and those preferring proactive removal of illegal content,[265] this Act remains in effect in Germany.[266]

In 2020, France attempted to pass "Lutte contre la haine sur internet" ("Fighting Hate on the Internet"), a law similar to the NetzDG, which requires online platforms to remove hate content within twenty-four hours of flagging and more serious illegal content, like child pornography, within one hour.[267] This "Avia Law," as it was known, was struck down by the French Constitutional Court on the ground of freedom of expression.[268] However, the French government recently indicated that it will seek greater control of hate speech by proposing a new bill which includes a procedure for intermediaries' responsibility, reminiscent of that which was declared unconstitutional.[269]

A recent proposed law in Poland provides a contrasting example, with social values differing markedly from those shown in the German and French legislation. The Polish government viewed the blocking of former President Trump's social media accounts as censorship and has

263. *Id.* art. 1, § 4(2).

264. *Id.* art. 1, § 1(3).

265. Section 3 deals with the Handling of complaints about unlawful content. Under 3(2) a "proactive" process for removal is set out. Under Section 3(2) 1, for instance, social media firms are required to "check whether the content reported in the complaint is unlawful or alternatively block it while Section 3(2) 4 require them to store as evidence cases of such removals. For a critique, *see, e.g.*, *Germany: Flawed Social Media Law*, HUMAN RIGHTS WATCH (Feb. 14, 2018), https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law#; For a background of NetzDG, *see* Heidi Tworek & Paddy Leerssen, *An Analysis of Germany's NetzDG Law* (Transatlantic High-Level Working Group on Content Moderation Online and Freedom of Expression, Working Paper, Apr. 15, 2019), https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

266. For a background, *see, e.g.*, Jenny Gesley, *Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech,* LIBRARY OF CONGRESS (2021), https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/.

267. Conseil constitutionnel [CC] [Constitutional Court] decsion No. 2020-801DC, June 18, 2020 (Fr.), http://www.iredic.fr/wp-content/uploads/2020/11/cc-18-juin-2020.pdf.

268. *Id.*; see also Manny Marotta, *France Constitutional Court Strikes Down Most of Online Hate Speech Law*, JURIST (June 20, 2020), https://www.jurist.org/news/2020/06/french-court-strikes-down-most-of-online-hate-speech-law/.

269. *See* Vie Publique, *Bill Consolidating Respect for the Principles of the Republic and the Fight Against Separatism*, REPUBLIQUE FRANCAISE, https://www.vie-publique.fr/loi/277621-loi-separatisme-respect-des-principes-de-la-republique.

moved to put regulations in place to "prevent abuse on the part of internet tycoons."[270] Citing the German law as a justifying example of legislation which imposes fines on social media platforms, the Polish proposal, rather than seek to clear hate speech, provides an avenue for users to complain wherever they are blocked by a social media provider.[271] If the complaint is rejected, the user can appeal to a special body, the "Freedom of Speech Council."[272] If the social media company ignores a ruling of the Council, they risk large fines.[273] While apparently aimed at protecting free speech, the Polish proposal also involves greater government oversight of social media firms, similar to the German and French regulation as well as the DSA.

Admittedly, these laws or proposals, either on the E.U. or domestic level, are not necessarily inconsistent with the Intermediary Immunity clause because the CDA 230-type arrangement under the USMCA and Japan-U.S. DTA protects online intermediaries against civil liabilities only.[274] These private liabilities, however, should be understood with public laws and constitutions in mind, as courts have to interpret these liabilities holistically to give effects to free speech.[275] We have seen divergent social values reproduced in different E.U. members' reactions to the growing threats to freedom of speech in the age of hate speech and misinformation. Even E.U. members are divided on an optimal model in striking a fine balance, let alone WTO members with diversified cultural backgrounds and heterogeneous interests, posing substantial difficulties to agreeing on a one-size-fits-all solution. This explains why none of the WTO members, other than the U.S., supported the

270. Magdelena Gad-Nowak & Marcin S. Wnukowski, *Polish Government to Pass Law That Will Allow it More Control Over the Internet Content and Legitimize Blocking Access to Certain Websites*, XI 172 NAT'L L. REV. 156 (2021); *see also* Michaela Cloutier, *Poland's Challenge to EU Directive 2019/790: Standing Up to the Destruction of European Freedom of Expression*, 125 DICK. L. REV. 161 (2020).

271. Michal Salajczyk, *Online Freedom of Speech Bill in Poland*, LEXOLOGY (blog Feb. 3, 2021) https://www.lexology.com/library/detail.aspx?g=3ae0a3cc-fdef-4d88-9f60-a91ea285fc41.

272. *Id.*

273. *Id.*; *see* Gad-Nowak & Wnukowski, *supra* note 270, at 156, 161.

274. However, the civil liability may intersect with other regulatory actions. A notice from the law enforcement authority in relation to illegal content may, for instance, trigger the "actual knowledge"—the prerequisite of the defamation liability.

275. In the UK, for instance, various defamation cases have been brought to the European Court of Human Rights to determine whether the English courts had appropriately balanced freedom of speech and other competing rights under the European Convention on Human Rights. Eur. Court of Human Rights, Guide on Article 10 of the European Convention on Human Rights: Freedom of Speech (Apr. 30, 2021). https://www.echr.coe.int/documents/guide_art_10_eng.pdf.

CDA 230 language in the E-Commerce Negotiation Text.[276] Thus, it is wise and pragmatic for countries to recognize the differences reflected in existing governance for online intermediaries' liabilities, rather than imposing the CDA 230-like text, which is rooted in the U.S. Constitution and has long attracted controversies.

IV. Conclusion

Traditionally, in an analog world with limited content providers and limited distribution channels, balancing freedom of expression and preventing harmful speech is fairly manageable. It is reasonable to expect the owners of bookstores—which cannot hold infinite collections—to know what they have in stock. Such an expectation, however, is not scalable to the digital context, where there are countless users uploading information through different intermediaries. CDA 230 was born in the 1990s as a tool to support online innovation and to safeguard free speech under the First Amendment. In a world without it, per Judge J. Harvie Wilkinson held in *Zeran v. America Online*, online intermediaries "would be faced with ceaseless choices of suppressing controversial speech [or] sustaining prohibitive liability."[277] This balance was struck in line with American values embedded in the Constitution; in fact, CDA 230 may have offered better protections than those available under the First Amendment.[278] Even outside of the United States, free speech is a universal right recognized in Article 19 of the International Covenant on Civil and Political Rights.[279] It matters at two levels. For individuals, free speech helps them develop as a person. Free speech is a cornerstone of a democratic society, allowing citizens to participate in public affairs through public debates, information sharing, and dialogue with others. While freedom of expression is a necessary precondition to the enjoyment of other rights—like voting rights, free assembly, and freedom of association—countries should however have their own pathways to achieve it. Different pathways reflect the economic, social, and political factors in progressing towards an optimal balance and rebalance between competing interests—reputation, for instance, is

276. WTO 2020 E-Commerce Negotiation Text, *supra* note 15, at 24.

277. Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997).

278. Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 Notre Dame L. Rev. Reflection 33, 36–37 (2019).

279. International Covenant on Civil and Political Rights art. 19(1), Dec. 16, 1966, S. Treaty Doc. No. 95-20, 999 U.N.T.S. 171 [hereinafter ICCPR].

explicitly recognized by Article 17 (2) of ICCPR.[280] While international trade law might play a role in furthering individuals' rights to share and receive information, thereby offering new opportunities for human rights law,[281] one may consider the challenges unique to each jurisdiction and its policy space.

The Intermediary Immunity clause, under the seemingly innocuous title "Interactive Computer Services," has gone far beyond economic concern per se and can only further complicate the already complex "*trade and*" issues.[282] The clause is so complex that even international human rights treaties can only set forth high-level instructions to manage it.[283] The Intermediary Immunity clause should be dropped from future trade negotiations while policymakers worldwide grapple with the critical challenges posed by online platforms and reconfigure their regulatory frameworks in the digital era.

280. *Id.* art. 17.2 ("Everyone has the right to the protection of the law against such interference or attacks.").

281. *See generally* Anupam Chander et al., *International Trade and Internet Freedom*, 102 AM. SOC'Y INT'L PROC. 37, 38 (2009).

282. *See, e.g.*, Joel P. Trachtman, *Institutional Linkage: Transcending "Trade and. . .",* 96 AM. J. INT'L. L. 77 (2002) (noting that [t]he general issue raised by most linkage claims is whether trade rules and environmental, labor, human rights, or other non trade rules should somewhat be combined at the WTO in a different way than they now are.) (emphasis original); see also David W. Leebron, *Linkages*, 96 AM. J. INT'L. L. 77 (2002) (observing that the linkage between "trade and. . ." is growing and this is driven by two forces. "First, more issues are now regarded as trade related in the narrow sense that the norms governing those issues affect trade. . .Second, an increasing number of substantive areas are the subject of international coordinated action or multilateral agreement." This is the case, [e]ven if conduct in such areas does not directly affect trade flows.").

283. On this score, the Council of Europe's Declaration expressly state that online platforms should act as per with the UN Guiding Principles on Business and Human Rights and the "Protect, Respect and Remedy" Framework to respect human rights of their users and affected parties in all their actions. When online platforms restrict access to third-party content based on a State order, the authorities "should ensure that effective redress mechanisms are made available and adhere to applicable procedural safeguards." Moreover, where platforms remove content based on their own service agreement, moreover, such "should not be considered a form of control that makes them liable for the third-party content for which they provide access." Recommendation CM/Rec (2018)2 of the Committee of Ministers to Member States on the Role and Responsibilities of Internet Intermediaries, Eur., Mar .07, 2018, Council of Eur.; s*ee also* U.N. H.R. *Joint Declaration on Freedom of Expression and Elections in the Digital Age* (Apr. 30, 2020).