Brooklyn Journal of International Law

Volume 47 | Issue 2 Article 1

12-30-2022

Breaking Down Digital Walls: The Interface of International Trade Law and Online Content Regulation through the Lens of the Chinese VPN Measure

Neha Mishra

BREAKING DOWN DIGITAL WALLS: THE INTERFACE OF INTERNATIONAL TRADE LAW AND ONLINE CONTENT REGULATION THROUGH THE LENS OF THE CHINESE VPN MEASURE

*Neha Mishra**

INTRODUCTION 360

I. ONLINE CONTENT REGULATION AND DIGITAL TRADE: UNDERSTANDING THE INTERLINKAGES 365

A. Impact on Digital Trade 366
B. Online Content Regulation as a Non-Tariff Barrier to Digital Trade 367
C. When Online Content Regulation Breaches GATS 369

II. INTERNATIONAL TRADE LAW AND ONLINE CONTENT REGULATION: FROM THE LENS OF THE CHINESE VPN MEASURE 370

A. The Measure at Issue: Notification of Chinese VPN Services ... 371
B. Chinese VPN Notification as a "Measure" under GATS 377
C. Identifying Chinese Commitments on VPN Services at the WTO 379
1. Scheduling Commitments on Digital Services 379
2. VPN Services: Telecommunications or Computer Services? 382
3. Chinese Commitments on VPN Services 386
D. Consistency of Chinese VPN Measure with GATS Obligations 388
1. Market Access 388
2. National Treatment 389
3. Domestic Regulation 393
4. GATS Telecommunications Annex 395
E. Justifying the Chinese VPN Measure under the GATS Art. XIV Exception 397
1. Relevance of GATS Exceptions 398
2. The Necessity of the Chinese VPN Measure under GATS art. XIV 404
3. Compliance with the General Exception Chapeau 408

---

* Assistant Professor, Geneva Graduate Institute. The author would like to thank Mira Burri, Andrew Mitchell, Shin-yi Peng and Tania Voon for helpful feedback on earlier drafts of the article, and Binit Agarwal for his excellent research assistance.

III. INTERNATIONAL TRADE LAW AND ONLINE CONTENT REGULATION: TOWARDS AN OPEN INTERNET 411

CONCLUSION 416

INTRODUCTION

The dramatic increase in global online content consumption, especially in the wake of the Covid-19 pandemic,[1] has increased both the desire and the public pressure on governments to regulate online content.[2] Online content regulation is not new; historically, governments have regulated online content to varying degrees to ensure compliance with public morality standards and censor content that is potentially politically sensitive or disruptive,[3] or to ensure compliance with intellectual property laws.[4] But the scale and the intensity of regulation today is

1. *Global Online Content Consumption Doubles in Wake of COVID*, WARC (Sept. 24, 2020), https://www.warc.com/newsandopinion/news/global-online-content-consumption-doubles-in-wake-of-covid/44130.

2. *See* DANIEL FUNKE & DANIELA FLAMINI, POYNTNER, A GUIDE TO ANTI-MISINFORMATION ACTIONS AROUND THE WORLD (2018), https://www.poynter.org/ifcn/anti-misinformation-actions/; Editorial Board, *Opinion: The Internet Became Less Free This Year — Again*, WASH. POST (Sept. 27, 2021, 4:11 PM), https://www.washingtonpost.com/opinions/2021/09/27/internet-freedom-decreases-again/; JACOB MCHANGAMA & JOELLE FISS, JUSTITIA, THE DIGITAL BERLIN WALL: HOW GERMANY (ACCIDENTALLY) CREATED A PROTOTYPE FOR GLOBAL ONLINE CENSORSHIP (2019), justitia-int.org/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf.

3. *See, e.g.*, for the ban on pornography, Info-Commc'ns Media Dev. Auth., Internet Code of Practice, art 4 (Nov. 1, 1997) (Sing.); Nada, *Lebanon Blocks Six Porn Sites, Sparks Fears of Further Censorship*, ADVOX GLOBAL VOICES (Sept. 10, 2014, 5:40 PM), https://advox.globalvoices.org/2014/09/10/lebanon-blocks-six-porn-sites-sparks-fears-of-further-censorship/; *see also* various examples discussed in YAMAN AKDENIZ, INTERNET CHILD PORNOGRAPHY AND THE LAW: NATIONAL AND INTERNATIONAL RESPONSES (2016).For regulations covering racially sensitive content, *see* Computer Information Network and Internet Security, Protection and Management Regulations (promulgated by the Ministry of Public Security, Dec. 30, 1997), art 4–6 (China); STRAFGESETZBUCH [PENAL CODE], § 86a, https://www.gesetze-im-internet.de/englisch_stgb/ (Ger.).

4. Peng Hwa Ang, *International Regulation of Internet Content: Possibilities and Limits*, *in* GOVERNING GLOBAL ELECTRONIC NETWORKS: INTERNATIONAL PERSPECTIVES ON POLICY AND POWER 305, 305 (William J. Drake & Ernest J. Wilson III eds., 2008).

unprecedented.[5] Governments today deploy a wide variety of regulatory and technological tools to regulate online content, including restricting and punishing circulation of fake news and disinformation,[6] political censorship,[7] and AI tools for preventing online hate and crimes.[8] Such regulations contrast with the fundamental architecture of the internet, which is agnostic to the content transferred through the network[9] and has traditionally been viewed as a platform to enable the free flow of information.[10]

---

5. *See 'Extremely Aggressive' Internet Censorship Spreads in the World's Democracies*, `MICH. NEWS (Nov. 17, 2020), https://news.umich.edu/extremely-aggressive-internet-censorship-spreads-in-the-worlds-democracies/; Editorial, *The Guardian View on Internet Censorship: When Access is Denied*, THE GUARDIAN (Jan. 1, 2020, 12:35 AM), https://www.theguardian.com/commentisfree/2020/jan/01/the-guardian-view-on-internet-censorship-when-access-is-denied.

6. *See generally* Rebecca K. Helm & Hitoshi Nasu, *Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation*, 21 HUM. RTS. L. REV. 302 (2021).

7. *See, e.g.*, Information Technology Act, 2000, § 69A (India); Law Concerning Electronic Information and Transactions, Law No. 11/2008, art. 40 (2008) (Indon.); *see also* Sarah Cook, *Analysis: The Clubhouse Affair: A Stark Reminder of China's Information Isolation*, *in* FREEDOM HOUSE, CHINA'S INFORMATION ISOLATION, NEW CENSORSHIP RULES, TRANSNATIONAL REPRESSION (2021), https://freedomhouse.org/report/china-media-bulletin/2021/chinas-information-isolation-new-censorship-rules-transnational; Justin Sherman, *Vietnam's Internet Control: Following in China's Footsteps?*, THE DIPLOMAT (Dec. 11, 2019), https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/.

8. Zachary Laub, *Hate Speech on Social Media: Global Comparisons*, COUNCIL ON FOREIGN RELS. (June 7, 2019, 3:51 PM), https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons.

9. *See* Simson Garfinkel, *The End of End-to-End?*, MIT TECH. REV. (July 1, 2003), https://www.technologyreview.com/2003/07/01/234174/the-end-of-end-to-end/#:~:text=The%20end%2Dto%2Dend%20principle,end%20operates%20on%20many%20levels.

10. GOOGLE, ENABLING TRADE IN THE ERA OF INFORMATION TECHNOLOGIES: BREAKING DOWN BARRIERS TO THE FREE FLOW OF INFORMATION 2 (2011), https://static.googleusercontent.com/media/www.google.com/en/us/google-blogs/pdfs/trade_free_flow_of_information.pdf; Blayne Haggart, *Platform Governance and the Clash of Values*, CIGI ONLINE (Jan. 10, 2022), https://www.cigionline.org/articles/platform-governance-and-the-clash-of-values/?utm_source=cigi_newsletter&utm_medium=email&utm_campaign=how-false-facts-led-to-the-capitol-riots.

This Article focuses on the complex interface of the law of the World Trade Organization (WTO)[11] and domestic online content regulation, using a case study of a measure regulating Virtual Private Networks (VPNs) in China. While this Article focuses on WTO law, the arguments set out below also apply to international trade law broadly. Section II explains why different tools of online content regulation, including restrictions imposed on digital services, apps and websites, or a complete ban on digital services or applications such as VPN services, can restrict digital trade in different ways. It remains contentious whether online content regulation should be treated as a non-tariff barrier, given that it is usually politically and culturally sensitive, especially contemporary policy concerns of disinformation and fake news. Nevertheless, such measures could implicate obligations contained in WTO treaties such as the *General Agreement on Trade in Services* (GATS)[12] and several other Free Trade Agreements (FTAs). In such scenarios, the exceptions available under GATS would be critical in justifying such measures.

Section III comprehensively studies the restriction on unlicensed VPN services in China (Chinese VPN measure)[13] to illustrate the interface of international trade law and domestic online content regulation in practice. This section argues that the Chinese VPN measure is potentially inconsistent with obligations on non-discrimination, domestic regulation, and certain obligations of the Telecommunications Annex of the GATS. China can, however, (at least provisionally) defend its measure under the general exception in GATS, which provides policy

---

11. The World Trade Organization or the WTO is a multilateral organization that regulates global trade through the administration of various international treaties signed between its Members. See https://www.wto.org/english/thewto_e/thewto_e.htm.

12. Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, annex 1B (General Agreement on Trade in Services) [hereinafter GATS]. The GATS is a treaty under the WTO that deals with trade in services among WTO members.

13. Gōngyè hé xìnxī huà bù guānyú qīnglǐ guīfàn hùliánwǎng wǎngluò jiē rù fúwù shìchǎng de tōngzhī
(工业和信息化部关于清理规范互联网网络接入服务市场的通知) [MIIT Notice on Cleaning Up and Regulating the Internet Access Service Market] (promulgated by the Ministry of Industry and Information Technology Telecom. Dept., Jan. 17, 2017, effective Jan. 22, 2017) Doc. No. 32 (China), https://www.chinalawtranslate.com/miit-notice-on-cleaning-up-and-regulating-the-internet-access-service-market/ [hereinafter Chinese VPN Measure].

space to WTO members (Members) to impose measures necessary for specific listed policy objectives such as protecting public morals, maintaining public order, and/or ensuring compliance with domestic laws.[14]

The case study on the Chinese VPN measure reveals various complexities of applying international trade law to online content regulations. First, the pre-internet age WTO rules, when applied to modern digital technologies, raise complex legal issues , such as: identifying the most relevant digital services sectors and commitments pertinent to the regulatory measure at issue; assessing "likeness" of foreign and domestic digital services and service providers; and examining whether a regulatory measure censoring online content meets the requirements of reasonableness, objectivity and impartiality consistent with obligations on domestic regulation. All these issues are not only challenging for trade tribunals to resolve, but also lead to legal uncertainty for governments and businesses alike.

Second, even if the Chinese VPN measure is found to be inconsistent with certain obligations in WTO law, the general exception provides significant policy space for governments to restrict unlicensed VPNs.[15] Some argue that WTO law could be a tool to counter measures such as online censorship measures that breach international human rights standards, and thereby defend the openness of the internet and preserve freedom of expression online.[16] While this approach may appear normatively attractive at first sight, a more judicious approach is that the WTO Panel (Panel) remains constrained and cautious in questioning the domestic values and policy goals informing the Chinese VPN measure. Rather, the Panel must predominantly focus on the design and implementation of the measure, including possible evidence regarding the measure being implemented in an arbitrary manner, or being used as a guise for protecting the domestic digital sectors in China. This approach would be consistent with the overall objective of WTO law and GATS, which recognizes that each member has the "right to regulate . . . to

14. See GATS, *supra* note 12, at art. XIV.

15. GATS, *supra* note 12, at art. XIV.

16. *See, e.g.*, Communication from the United States, *Joint Statement on Electronic Commerce Initiative*, WTO Doc. INF/ECOM/5 (Mar. 25, 2019) [hereinafter *Joint Statement on Electronic Commerce Initiative*]; Anupam Chander, *International Trade and Internet Freedom*, 102 PROCEEDINGS OF THE ASIL ANNUAL MEETING 37 (2008).

meet [their] national policy objectives."[17] Further, it would prevent panels from overstepping the boundaries of international trade agreements and making unpopular decisions. It may even lead to deliberate defiance by Members. Finally, this Article argues that in the absence of international consensus on norms and tools of internet censorship/content regulation,[18] trade tribunals are not well-placed to examine the normative basis of such measures.

Based on the case study in Section III, Section IV argues that international trade law agreements should not form the basis to scrutinize or criticize the domestic (and perhaps unique) cultural, social, religious, and political values that inform online content regulation. This does not, however, mean that international trade law has no role. In evaluating the design and implementation of such regulations, trade disciplines might be effective in weeding out measures which are deliberately protectionist and arbitrary. This conclusion also allays the fear that several countries have regarding how international trade agreements interfere with their ability to regulate the domestic internet.[19] Thus, the paper cautions against overly optimistic proposals to use international trade agreements to enable an open internet and the free flow of information.[20] Evolving norms on global data and digital governance, including online censorship, however, could be influential in the long run in reducing online content regulations that constrain digital trade.

Section V concludes that international trade law can discipline certain protectionist aspects of domestic online content regulations but cannot necessarily guarantee an open and free internet by completely curtailing such measures, even where they have an adverse effect on human rights. In the long run, such policy goals may be addressed (at least to some extent) in other international, transnational, and even multistakeholder internet

17. GATS, *supra* note 12, at pmbl.

18. *See* JONATHAN ZITTRAIN, ROBERT FARIS, HELMI NOMAN, JUSTIN CLARK, CASEY TILTON & RYAN MORRISON-WESTPHAL, INTERNET MONITOR, THE SHIFTING LANDSCAPE OF GLOBAL INTERNET CENSORSHIP 3–5 (2017), https://dash.harvard.edu/bitstream/handle/1/33084425/The%20Shifting%20Landscape%20of%20Global%20Internet%20Censorship-%20Internet%20Monitor%202017.pdf.

19. *See, e.g.*, Statement by the African Group, *The Work Programme on Electronic Commerce*, WTO Doc. JOB/GC/144 (Oct. 20, 2017).

20. *See, e.g.*, *Joint Statement on Electronic Commerce Initiative*, *supra* note 16.

governance and human rights bodies. Meanwhile, behind the rising digital walls, the tension between internet openness and domestic online regulation will inevitably continue to play out in international trade law. The best way for trade bodies to deal with this tension is to remain both pragmatic and cautious in trying to break down these digital walls.

I. ONLINE CONTENT REGULATION AND DIGITAL TRADE: UNDERSTANDING THE INTERLINKAGES

The tools used by governments to censor and regulate online content can vary considerably, depending on their governance capacity and the degree to which the government wants to control information flows in the online environment. The turn to digital authoritarianism in several parts of the world has also led to more vigorous enforcement of online content regulations, especially to monitor politically and socially sensitive content.[21]

Governments often impose an outright ban on digital services, platforms, and websites that host or allow circulation of prohibited or delicate content.[22] Online content can also be regulated by imposing specific requirements on platforms and social media to remove content based on government guidelines or directions.[23] Other mechanisms for blocking online content could be selective filtering or degrading the performance of websites containing offensive content.[24]

Finally, governments sometimes rely on indirect tools such as restricting the availability of VPN services, which allow people to circumvent government restrictions on online content.[25] The latter presents a sophisticated and nuanced example of

---

21. ADRIAN SHAHBAZ, FREEDOM HOUSE, FREEDOM ON THE NET 2018: THE RISE OF DIGITAL AUTHORITARIANISM 1-19 (2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

22. *See generally* Peng Hwa Ang, *How Countries Are Regulating Internet Content*, INTERNET ' (June 25, 1997), https://www.isoc.org/inet97/proceedings/B1/B1_3.HTM.

23. *See, e.g.*, *Government Requests to Remove Content*, GOOGLE TRANSPARENCY REPORT, https://transparencyreport.google.com/government-removals/overview?hl=en (last visited Nov. 25, 2022); *see generally* OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY (Giancarlo Frosio ed., 2020).

24. Joseph Hall, Michael Aaron, Ben Jones & Nick Feamster, *A Survey of Worldwide Censorship Techniques*, INTERNET ' TASK FORCE 7 (May 25, 2018), https://tools.ietf.org/id/draft-hall-censorship-tech-05.html#rfc.section.4.

25. *See* HUM. RTS. WATCH, HOW CENSORSHIP WORKS IN CHINA: A BRIEF OVERVIEW 5 (2006), https://www.hrw.org/reports/2006/china0806/3.htm.

regulation of online content via the regulation of a technology, and is often more effective in restricting access to online content as compared to more traditional online censorship or filtering methods.[26] This section explains how different forms of online content regulation impact digital trade and whether they should be considered as non-tariff barriers.

A. Impact on Digital Trade

Different forms of online content regulation restrict digital trade in different ways.[27] For instance, an express ban on specific or all foreign digital services (e.g., social media platforms) will expectedly prevent any foreign suppliers from operating in that market. If restrictions on foreign digital services and service providers were replicated across several countries, it could lead to the eventual fragmentation of markets globally, which in turn would also affect growth and innovation in the digital sector,[28] and intensify cybersecurity risks.[29]

Measures that specifically protect or promote domestic alternatives (e.g., domestic social media platforms, domestic payment systems, etc.) may also be seen as providing an unfair advantage to domestic firms, when the country imposing such measures has committed to opening these sectors to foreign competition under various international trade treaties. Several industry experts believe that Chinese companies such as Baidu, Alibaba and Tencent were only able to flourish because China restricted availability of their US competitors such as Google, Amazon, Twitter, and Facebook through stringent internet regulation.[30]

---

26. Other countries that have considered similar restrictions on VPN include Iran, Russia, Syria, Pakistan, and Turkey.

27. *See generally* Google Inc., *Enabling Trade in the Era of Information Technologies: Breaking Down*
Barriers to the Free Flow of Information, 8 TRANSNAT'L DISP. MGMT. 8-11 (2011), https://
www.transnational-dispute-management.com/article.asp?key=1658.

28. *See What's at Stake in Digital Fragmentation? Q&A with Zoom's Josh Kallmer*, CTR. FOR LONG-TERM CYBERSECURITY (Nov. 2, 2020), https://cltc.berkeley.edu/2020/11/02/whats-at-stake-in-digital-fragmentation/.

29. EY, *The Fragmentation of Everything*, MIT TECH. REV. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013038/the-fragmentation-of-everything/.

30. *See, e.g.*, *Censorship as a Non-Tariff Barrier to Trade*, *Hearing Before the Subcomm. on Int'l Trade, Customs, and Glob. Competitiveness* 116th Cong. 3 (2020) (testimony of Nigel Corey, Assoc. Dir., Trade Pol'y Info. Tech. &

Further, recent years have seen governments imposing vaguely worded laws and regulations setting out various requirements for digital service providers, including licensing and compliance requirements.[31] Such regulations can lead to business uncertainty and could be especially disadvantageous for foreign firms operating in those markets.

From a broader policy perspective, online content regulation, especially when it takes the form of Domain Name System-based blocking,[32] and other kinds of invasive filtering mechanisms, interferes with the seamless and open architecture of the internet and can thus be seen as a precursor to internet fragmentation.[33] This fragmentation could also entail human rights violations, including reduced access to information and a breach of freedom of expression.[34] Such concerns, however, do not fall within the conventional boundaries of international trade law unless the relevant regulation is also trade-restrictive in nature.

B. Online Content Regulation as a Non-Tariff Barrier to Digital Trade

For several years, certain countries, especially the United States of America (US), have argued that online content regulation, especially censorship measures, can be barriers to digital trade. For example, the 2016 National Trade Estimate Report, issued by the United States Trade Representative (USTR),

---

Innovation Found.), https://www2.itif.org/2020-censorship-non-tariff-barrier-trade.pdf. [hereinafter ITIF].

31. *Content Regulation in the Digital Age* (Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression by the Association for Progressive Communications), OHCHR (Feb, 2018), https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/APC.pdf.

32. INTERNET SOC'Y, INTERNET SOCIETY PERSPECTIVES ON INTERNET CONTENT BLOCKING: AN OVERVIEW 19–20 (2017), https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf.

33. WILLIAM J. DRAKE, VINTON G. CERF, & WOLFGANG KLEINWÄCHTER, WORLD ECON. F., INTERNET FRAGMENTATION: AN OVERVIEW 34 (2016), https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

34. Simon K. Zhen, *Combating Censorship in China: Forcing China's Hand Through the WTO and Collective Action*, 53 CORNELL INT'L L. J. 731, 734 (2020).

clearly set out the Great Firewall of China[35] as a trade barrier for US companies:

> Over the past decade, China's filtering of cross-border Internet traffic has posed a significant burden to foreign suppliers, hurting both Internet sites themselves, and users who often depend on them for their businesses. Outright blocking of websites appears to have worsened over the past year, with 8 of the top 25 most trafficked global sites now blocked in China. Much of the blocking appears arbitrary; for example, a major home improvement site in the United States, which would appear wholly innocuous, is typical of sites likely swept up by the Great Firewall.[36]

A similar position was taken by the USTR in several subsequent reports.[37] In 2020, the US Senate also held a hearing on examining the role of censorship as a non-tariff barrier to trade, predominantly focusing on a variety of internet regulations in China.[38] Other countries have not been as openly vocal regarding the trade restrictive impact of online content regulation, although several experts argue that at least some online censorship measures are an intelligently disguised barrier to digital trade.[39] For digitally advanced countries such as China, online content regulation may further enhance the political prowess of the Chinese government as a cyber super-power.[40]

On the other hand, although online content can sometimes result in a trade-restrictive impact, this is incidental to the necessary and legitimate domestic regulation of apps or websites that

---

35. Geremie R. Barme & Sang Ye, *The Great Firewall of China*, WIRED (June 1, 1997, 12:00 PM), https://www.wired.com/1997/06/china-3/ (The Great Firewall of China refers to various measures taken by the Chinese government to regulate the internet in China, including monitoring and censoring online content that is available within China).

36. AMBASSADOR MICHAEL B.G. FROMAN, OFF. OF U.S. TRADE REP., 2016 NATIONAL TRADE ESTIMATES REPORT ON FOREIGN TRADE BARRIERS 91 (2016).

37. *See, e.g.*, OFF. OF U.S. TRADE REP., 2017 NATIONAL TRADE ESTIMATES REPORT ON FOREIGN TRADE BARRIERS 90 (2017).

38. *See generally Censorship as a Non-Tariff Barrier to Trade: Hearing Before the S. Subcomm. on Int'l Trade, Customs, and Glob. Competitiveness of the Comm. on Fin.*, 116th Cong. (2020).

39. ITIF, *supra* note 30, at 3; Zhen, *supra* note 34, at 731; *see generally* Nikolai Topornin, Darya Pyatkina & Yuri Bokov, *Government Regulation of the Internet as Instrument of Digital Protectionism in Case of Developing Countries*, J. INFO. SCI. 1–14 (2021).

40. ITIF, *supra* note 30, at 4.

could potentially host illegitimate content such as child pornography, fake news, or blasphemous content. Therefore, it is important to preserve the ability of governments to regulate digital content providers and hosting platforms in the most effective and least trade-restrictive manner.

C. When Online Content Regulation Breaches GATS

Where an online content regulation measure restricts digital trade, whether deliberately or incidentally, it can breach different obligations contained in GATS and other international trade agreements. For instance, governments may restrict foreign websites providing certain forms of content but allow domestic companies to provide similar content, because local platforms are arguably easier to monitor via domestic laws. This kind of discriminatory treatment against foreign websites or services can favor local companies by protecting them from foreign competition and could violate non-discrimination principles.[41]

Another example involving a breach of the non-discrimination obligation is when a government targets digital services from a specific country on the grounds of regulating illegitimate content while allowing import of digital services of other trading partners, who provide access to similar online content. Further, in countries where certain kinds of content is expressly banned (e.g., pornographic materials), any foreign supplier that hosts or provides such content is potentially prohibited from accessing those domestic markets.[42] Such a measure can be discriminatory if certain domestic suppliers are still able to provide such content irrespective of the ban. For example, although Facebook has been blocked in China since 2009, a variety of domestic platforms such as WeChat provide comparable social media services.

---

41. *See, e.g.*, Li Yuan, *A Generation Grows Up in China Without Google, Facebook or Twitter*, N.Y. TIMES (Aug. 6, 2018), https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html (The principle of non-discrimination means that a country cannot discriminate against like services and service providers from other countries or differentiate between like services and service providers between different foreign countries) .

42. Fredrik Erixon, Brian Hindley & Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law* 8–9, (Eur. Ctr. for Int'l Pol. Econ., Working Paper No. 12/2009, 2019), https://ecipe.org/wp-content/uploads/2014/12/protectionism-online-internet-censorship-and-international-trade-law.pdf.

Additionally, licensing and other compliance conditions imposed on foreign digital service providers may be inconsistent with the obligations on domestic regulation under GATS Article VI.[43] As discussed in greater detail below in the context of the Chinese VPN measure, the breach of obligations under GATS depends on the specific measure, the sectors affected by the measure, and the relevant commitments in those specific sectors in the member's GATS Schedule.[44]

Even if a measure pertaining to online content regulation is inconsistent with a member's obligations under the GATS or other international trade agreements, the member can argue that the measure is justifiable under the exceptions contained in the treaty.[45] For instance, a member could argue that an express ban on a specific digital platform is necessary to protect public morals,[46] to maintain public order,[47] or to ensure compliance with domestic laws.[48] Therefore, in striking a balance between promoting digital trade liberalization, and protecting a country's right to regulate, the exceptions play a significant and central role.[49]

II. INTERNATIONAL TRADE LAW AND ONLINE CONTENT REGULATION: FROM THE LENS OF THE CHINESE VPN MEASURE

This section examines whether the Chinese VPN measure is consistent with China's obligations under the WTO treaties. This case study aims to illustrate the interface of WTO law and online content regulation by providing a systematic account of how obligations in trade agreements apply to the Chinese VPN

43. GATS, *supra* note 12, at art. XIV.

44. See Section IIIC1.

45. For instance, measures can be justified under GATS Article XIV.

46. For instance, a measure banning the circulation of pornographic content can be defended under the public morals exception.

47. For instance, a measure that monitors or prohibits circulation of fake news may be justified on grounds of public order as it can potentially lead to violence or communal disharmony.

48. For instance, a measure aimed at protecting certain vulnerable groups of people from online harassment, including by monitoring sensitive content, can constitute a measure necessary to ensure compliance with domestic anti-discrimination laws.

49. Section III explains how the general exception in GATS applies specifically in the context of the Chinese VPN measure, and thereafter evaluate the broader policy implications of the interface of international trade law and domestic online regulation.

measure. Thereafter, Section IV considers the prospects and limits of international trade agreements in contributing to a free and open internet. Limited information is publicly available on the implementation of this measure, particularly government reports. Therefore, the assessment below is based on publicly available information. A broader discussion of the complex regime for internet regulation/censorship in China is outside the scope of this Article.[50]

Section IIA explains the main requirements prescribed in the notification banning unlicensed VPN measures in China. Section IIB argues why this notification constitutes a "measure" under GATS. Section IIC explains why China's commitments in its WTO GATS Schedule can be interpreted to cover VPN services. Section IID explains why the Chinese VPN measure is inconsistent with obligations on national treatment and domestic regulation and potentially also violates the GATS Telecommunications Annex. Section IIE argues that the Chinese VPN measure can be provisionally justified under the general exception contained in GATS art. XIV(a). However, if a complainant can adduce evidence that the implementation of this measure vis-à-vis foreign VPN services and service suppliers is arbitrary or discriminatory, then the measure could be inconsistent with the GATS art. XIV chapeau.[51]

A. The Measure at Issue: Notification of Chinese VPN Services

VPN services provide a private network (enabled by encryption) for point-to-point connection over the public network of the

---

50. *See, e.g.*, Henry S. Gao, *Data Regulation with Chinese Characteristics*, *in* BIG DATA AND GLOBAL TRADE LAW 245–67 (Mira Burri ed., 2021), https://www.cambridge.org/core/books/big-data-and-global-trade-law/data-regulation-with-chinese-characteristics/2539ECBA4499D555BD8206948AD8F4BB; Kristina M. Reed, *From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce*, 13 TRANSNAT'L LAW. 451 (2000); Cynthia Liu, *Internet Censorship as a Trade Barrier: A Look at the WTO Consistency of the Great Firewall in the Wake of the China-Google Dispute*, 42 GEO. J. INT'L L. 1199, 1207–11 (2011); Alex Wyatt, *The Global Economy and the On-line World: Consequences of the WTO Accession on the Regulation of the Internet in China*, 3 MELB. J. INT'L L. 436 (2002); Natalie E. Sammarco, *The Great Firewall and the Perils of Censorship in Modern China*, YALE J. INT'L AFFS. (2013), https://www.yalejournal.org/publications/the-great-firewall-and-the-perils-of-censorship-in-modern-china; Zhen, *supra* note 34, at 734–46.

51. *See* Section IIIE.

internet.[52] This network enables anonymity and privacy of communications while acting like the point-to-point network connection provided by the public internet.[53] VPNs are not per se illegal in China but are heavily regulated under various domestic frameworks, as explained below. Businesses cannot generally set up or lease a private circuit such as a VPN service without approval from the telecommunications regulator.[54]

VPN services used for domestic network connections are classified as Value-Added Telecommunication Services (VATS), while VPN services provided for cross-border network connections are classified as Basic Telecommunications Services (BTS).[55] This difference in classification has regulatory implications. Any services that qualify as BTS, such as VPN services for cross-border network connections, are regulated more stringently in China, including the requirement to obtain a permit from the Ministry of Industry and Information Technology (MIIT) to provide the service.[56] In contrast, the use of any networks classified as VATS, such as VPNs providing domestic network connections, only need to be notified to the MIIT.[57]

---

52. Steve Symanovich, *What is a VPN?*, NORTON (Feb. 24, 2022), https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html.

53. Alexander S. Gillis, *VPN (virtual private network)*, TECHTARGET (Sept., 2021), https://www.techtarget.com/searchnetworking/definition/virtual-private-network.

54. These requirements are set out in Zhonghua renmin gonghe guo jisuanji xinxi wangluo guoji liangwang guanli zhanxing guiding (中华人民共和国计算机信息网络国际联网管理暂行规定) [Provisional Regulations of the People's Republic of China on the Management of International Networking of Computer Information Networks] (promulgated by the State Council, Feb. 1, 1996, effective Feb. 1, 1996) (Lawinfochina); Guoji tongxiin churukou ju guanli banfa (**国际通信出入口局管理**办**法**) [Measures on the Administration of International Communication Accesses] (promulgated by the Ministry of Information Industry, Mar. 14, 2002, effective Oct. 1, 2002) CLI.4.40342(EN) (Lawinfochina).

55. Sven-Michael Werner, *Network Connection and VPN—What MNCs Need to Learn for Legally Connecting Headquarters, Subsidiaries, Branches and Employees Within or Outside China?*, BIRD&BIRD (Dec. 30, 2020), https://www.twobirds.com/en/news/articles/2020/china/network-connection-and-vpn [citing to MIIT Classified Catalogue of Telecommunications Services (2015)].

56. *Id.*

57. Guó jì tōng xìn chū rù kǒu jú guǎn lǐ bàn fǎ (国际通信出入口局管理办法) [Regulation on Administration of International Communications Gateway Exchange Procedures] (promulgated by the Ministry of Industry and Information Technology, June 26, 2002, effective Oct. 1, 2002), arts. 5–6 (China).

Cross-border VPN services can only be used for internal corporate or business purposes.[58] Therefore, any company requiring access to VPNs for a cross-border network connection can theoretically lease the service from licensed operators. Currently, licensed cross-border VPN services are predominantly provided by three domestic telecom companies: China Telecom, China Unicom and China Mobile.[59] A Chinese venture of the British company, BT Group PLC, has also obtained permission to provide VPN services in China, but this is limited to domestic network services.[60] Industry consultations also indicate that MIIT often requires companies to obtain a license for domestic network connection (e.g., between different offices in China), especially when it considers that the connection relates to non-commercial purposes.[61] The main regulatory focus of the Chinese government, however, has been on unlicensed or unauthorized VPN services used for cross-border connections.[62]

The measure that is examined in this case study, namely the Chinese VPN measure, is contained in the *MIIT Notice on Cleaning up and Regulating the Internet Access Market*.[63] The notification states that it is aimed at investigating and reducing "illegal activities" on the internet, more specifically in "internet data centres, internet access services and content distribution network markets," for example, businesses without permits and subleasing of internet services.[64] Further, the notification aims to strengthen the "management of business permits and access resources, and harden the management of cybersecurity" and "to maintain a fair and orderly market, and promote the healthy development of the sector."[65] Several of the requirements set out

58. Werner, *supra* note 55.

59. Jon Russell, *China's Mobile Operators Are Reportedly Being Told to Ban All Use of VPNs*, TECH CRUNCH (July 10, 2017, 11:43 AM), https://techcrunch.com/2017/07/10/china-vpn-ban/.

60. Winston Qiu, *BT Obtains Nationalwide Telecom Licenses in China*, SUBMARINE NETWORKS (Jan. 25, 2019), https://www.submarinenetworks.com/en/insights/bt-obtains-nationalwide-telecom-licenses-in-china-updated.

61. Werner, *supra* note 55.

62. *Id.*

63. Chinese VPN Measure, *supra* note 13.

64. Chinese VPN Measure, *supra* note 13, ¶ I.

65. *Id.*

in the Chinese VPN measure reflect previous laws and regulations on VPN access.[66]

The Chinese VPN measure requires all service suppliers operating cross-border network connections via VPN services in China to obtain authorization from the Chinese government.[67] The notification states that VPN services "cannot be created or hired without such permission even if it is to conduct cross-border business activities."[68] Further, it imposes additional obligations on service suppliers to create "a centralized user archive," and ensure that "the terms of use of those lines are limited to internal office use."[69] The notification also prohibits VPN services that "connect to domestic or overseas data centers or operations platforms to conduct telecommunication operations business activities."[70] Thus, only authorized VPN services can be used for intra-company communications and without connecting to overseas data centers. This measure also enables the government to track all VPN users in China through the centralized user archive.[71]

According to various press reports, this notification was not intended to ban VPN services in China completely; rather, it was aimed at ensuring that only authorized VPN services are used in China.[72] The MIIT also clarified that this Notice does not prevent foreign companies requiring access to cross-border network services to rent them from licensed operators who provide such

66. BEITEN BURKHARDT, CHINA: DATA PROTECTION & LOCALISATION, CYBER SECURITY LAW, VPN AND ENCRYPTION 2–3 (2018), https://www.advant-beiten.com/sites/default/files/downloads/BB%20BR-Flyer%20A5%20China-Data%20Protection%20en.pdf.

67. Chinese VPN Measure, *supra* note 13, ¶ II(1).

68. Chinese VPN Measure, *supra* note 13, ¶ II(4).

69. *Id.*

70. *Id.*

71. Yuxi Wei, *China's New Cybersecurity Regulations: Analyzing the Ban on VPN Services*, UNIV. OF WASH.: THE HENRY M. JACKSON SCH. OF INT. STUD. (Apr. 12, 2017), https://jsis.washington.edu/news/chinas-new-cybersecurity-regulations-analyzing-ban-vpn-services/.

72. *See* Zhang Zihan, *Foreign-Run VPNs Illegal in China: Govt*, THE GLOB. TIMES (Dec. 14, 2012, 1:15 AM), http://www.globaltimes.cn/content/750158.shtml; Josh Ye, *China Tightens Great Firewall by Declaring Unauthorised VPN Services Illegal*, S. CHINA MORNING POST (Jan. 23, 2017, 1:15 PM), https://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall; Paul Bischoff, *Green VPN is shutting down, try these alternatives*, COMPARITECH (July 2, 2017), https://www.comparitech.com/blog/vpn-privacy/green-vpn-alternatives/.

international gateways.[73] As per several press reports, however, immediately after the measure came into effect in 2017, a majority of mobile and local VPNs became largely unavailable in China.[74] For example, Apple, Amazon and GreenVPN removed access to all VPN services immediately after the publication of the notification.[75] To date, availability of VPN services in China remains largely erratic and limited.[76]

Systematic evidence is not publicly available on the effects and implementation of the Chinese VPN measure. Press reports indicate that since the publication of the notification, cross-border network connections via VPN services have remained largely unavailable except for the expensive services offered by three state-owned enterprises telecommunications companies, namely China Telecom, China Mobile, and China Unicom.[77]

Recent press reports also indicate that during the Covid-19 pandemic, the Chinese government was especially stringent in

---

73. Li Xiyin, 工信部否认要运营商禁止个人VPN业务：规范对象是无资质者, [The Ministry of Industry and Information Denies That It Wants Operators to Ban Personal VPN Services: The Target of the Regulation is the Unqualified], THE PAPER (July 12, 2017, 4:40 PM), https://www.thepaper.cn/newsDetail_forward_1730060.

74. James Palmer, *China Is Trying to Give the Internet a Death Blow*, FOREIGN 'Y (Aug. 25, 2017, 1:30 PM), https://foreignpolicy.com/2017/08/25/china-is-trying-to-give-the-internet-a-death-blow-vpn-technology/.

75. Liat Clark, *China Aims to Close Holes in Its Firewall by Banning VPNs*, WIRED (Jan. 23, 2017, 3:00 PM), https://www.wired.co.uk/article/china-aims-to-close-holes-in-its-firewall-by-banning-vpns; Gao Feng, *Amazon's China Partner Bans Use of VPNs by Customers Amid Ongoing Clampdown*, RADIO FREE ASIA (Aug. 2, 2017), https://www.rfa.org/english/news/china/vpn-amazon-08022017135851.html; Tim Bradshaw, *Apple Drops Hundreds of VPN Apps at Beijing's Request*, FIN. TIMES (Nov. 21, 2017), https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc; Bischoff, *supra* note 72.

76. Arjun Kharpal & Kif Leswing, *Apple's New Privacy Feature, Designed to Mask Users' Internet Browsing, Won't Be Available in China*, CNBC (June 7, 2021, 11:09 PM, updated June 8, 2021, 1:31 AM), https://www.cnbc.com/2021/06/08/apple-wwdc-new-private-relay-feature-will-not-be-available-in-china.html.

77. *See* Leonhard Weese, *What Does China's VPN Ban Really Mean*, FORBES (Jan. 25, 2017, 1:33 AM), https://www.forbes.com/sites/leonhard-weese/2017/01/25/what-does-chinas-vpn-ban-really-mean/#52506f5d50e3>; Wei, *supra* note 71.

curtailing the supply of unlicensed VPN services.[78] Some experts have commented that the recent draft guidelines entitled "Network Data Security Management Regulations,"[79] which imposes new penalties for any person bypassing government-imposed censorship via the firewall, would have "far-reaching implications" for VPN service providers in China and foreign companies relying on such services.[80] In Beijing, the local government approved a plan allowing foreign companies to offer VPN services, provided that they own a maximum of 50 percent in JVs with local partners.[81] Since this development is relatively recent, it is unknown how this plan will be implemented in practice.

By banning the use of unlicensed VPN services for cross-border network connections and restricting the use of licensed VPN services for corporate purposes, the Chinese VPN measure acts as an indirect tool of online content regulation. Expectedly, measures restricting VPN services impact accessibility to online content and interfere with the seamless and open architecture of the internet. In fact, keeping the Chinese internet "clean" or free from illegal, offensive, and immoral content is at the heart of this measure alongside other cybersecurity-related

---

78. Grady McGregor, *China Deploys A Favorite Weapon in the Coronavirus Crisis: A Crackdown on VPNs*, FORTUNE, (Feb. 25, 2020, 7:00 PM), https://fortune.com/2020/02/25/coronavirus-china-vpn/; Yuan Yang, *China Stifles Foreign Internet to Control Coronavirus Coverage*, FIN. TIMES, (Feb. 17, 2020), https://www.ft.com/content/0aa9c0ec-517a-11ea-8841-482eed0038b1.

79. *See specifically*, Article 41: The state establishes a cross-border data security gateway to block the dissemination of information originating outside the territory of the People's Republic of China and prohibited from being published or transmitted by laws and administrative regulations.

80. Elles Houweling, *China Tightens Its Choke Hold on Great Firewall Piercing VPNs*, VERDICT (Nov. 16, 2021), https://www.verdict.co.uk/new-data-rules-in-china-could-see-individuals-punished-for-using-a-vpn/; *see also* Lester Ross, Kenneth Zhou & Tingting Liu, *China Publishes Draft Regulations on the Administration of Network Data Security*, WILMERHALE (Dec. 6, 2021), https://www.wilmerhale.com/en/insights/client-alerts/20211206-china-publishes-draft-regulations-on-the-administration-of-network-data-security; Henry Gao (@henrysgao), TWITTER (Nov. 14, 2021, 09:52 AM), https://twitter.com/henrysgao/status/1459806478886309890.

81. Anthony Spadafora, *China Wants to Open Up Its VPN Market Again*, TECH RADAR (Sept. 15, 2020), https://www.techradar.com/au/news/china-wants-to-open-up-its-vpn-market-again; He Shujing & Ding Yi, *Beijing Gets Green Light to Open VPN Services to Foreign Investors*, CAIXIN GLOB. (Oct. 19, 2021, 8:31 PM), https://www.caixinglobal.com/2021-10-19/beijing-gets-green-light-to-open-vpn-services-to-foreign-investors-101788751.html.

objectives.[82] This measure can also be closely linked to China's goal of achieving internet or cyber sovereignty,[83] a policy objective it has repeatedly asserted in several international platforms.[84]

B. Chinese VPN Notification as a "Measure" under GATS

The first question is whether VPNs constitute services under GATS. A circular definition of service is set out under GATS as "any service in any sector except services supplied in the exercise of governmental authority."[85] Further, GATS applies "to measures by Members affecting trade in services,"[86] where trade in services is defined as the "supply of a service" through different modes of delivery.[87] Under GATS, "supply of a service" is defined very broadly to include "production, distribution, marketing, sale and delivery of a service."[88] VPNs are software that allow confidential connectivity to the internet using sophisticated encryption techniques over the public internet. Thus, despite the ambiguity in the definition of service under GATS, VPNs can be considered services.

The next question is whether the Chinese VPN measure is a measure that affects trade in services. The word "measure" has been defined very broadly under GATS art. XXVIII(a) as "any measure by a member, whether in the form of a law, regulation, rule, procedure, decision, administrative action, or any other form."[89] In *Argentina – Financial Services*, the WTO Appellate Body (AB) held that the words "any measure" and "any other form" in Article XXVIII(a) imply that there is no "a priori

82. See further discussion in Section IIIE1.

83. HARRIET MOYNIHAN & CHAMPA PATEL, CHATHAM HOUSE, RESTRICTIONS ON ONLINE FREEDOM OF EXPRESSION IN CHINA 2 (2021), https://www.chathamhouse.org/sites/default/files/2021-03/2021-03-17-restrictions-online-freedom-expression-china-moynihan-patel.pdf.

84. *See generally* Jinghan Zeng, Tim Stevens & Yaru Chen, *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty,"* 45 POL. & POL'Y 432 (2017).

85. GATS, *supra* note 12, at art. I:3(b).

86. GATS, *supra* note 12, at art. I:1.

87. GATS, *supra* note 12, at art. I:2.

88. GATS, *supra* note 12, at art. XXVIII(b).

89. GATS, *supra* note 12, at art. XXVIII(a).

exclusion of the type or form that a measure may take under GATS."[90] In *US – Corrosion Resistant Steel Sunset Review*, the AB held that "any act or omission attributable to a Member can be a measure of that Member for purposes of dispute settlement proceedings."[91] Further, even unwritten practices of the government, such as a norm or practice, can constitute a measure.[92] On rare occasions, panels have considered certain discretionary government actions, even where no binding measures existed."[93]

Given the broad definition of measure under GATS art. XXVIII(a), the notification on Chinese VPN services can be considered a "measure." Although the notification only requires removal of unlicensed VPN services, consistent with previous laws and regulations and aligned with China's broader cybersecurity regulation framework,[94] all foreign service suppliers immediately removed VPN services from their Chinese application stores. Such a response by foreign companies suggests that the measure was binding or, at least, that the government demanded that all foreign companies act upon the notification.[95] This cannot be firmly concluded from any government reports, however, for the purposes of this paper, it is assumed that this notification was enforced by the government.

---

90. Appellate Body Report, *Argentina – Measures Relating to Trade in Goods and Services*, Annex on Financial Services ¶ 6.259, WTO Doc. WT/DS453/AB/R (adopted May 9, 2016) [hereinafter Argentina – Financial Services AB Report].

91. Appellate Body Report, *United States – Sunset Review of Anti-Dumping Duties on Corrosion-Resistant Carbon Steel Flat Products from Japan*, ¶ 81, WTO Doc. WT/DS244/AB/R (adopted Jan. 9, 2004).

92. Appellate Body Report, *United States – Continued Existence and Application of Zeroing Methodology*, ¶ 198, WTO Doc. WT/DS350/AB/R (adopted Feb. 19, 2006).

93. *See, e.g.*, Panel Report, *United States – Sections 301–310 of the Trade Act of 1974*, ¶ 7.53–7.54, WTO Doc. WT/DS152/R (adopted Jan. 27, 2000); Panel Report, *China – Measures Affecting the Protection and Enforcement of Intellectual Property Rights*, ¶ 7.359–7.367, ¶ 7.393–7.394, WTO Doc. WT/DS362/R (adopted Mar. 20, 2009).

94. *See generally* Gao, *supra* note 50.

95. *See, e.g.*, Russell, *supra* note 59.

C. Identifying Chinese Commitments on VPN Services at the WTO[96]

The VPN measure seems to favor domestic VPN suppliers, especially those owned by state-owned enterprises, which may affect foreign service suppliers and potentially violate market access and non-discrimination obligations, specifically national treatment, in GATS.[97] However, before assessing whether the Chinese VPN measure is inconsistent with these international trade obligations, a panel needs to ascertain whether China has inscribed any commitments on national treatment and market access on VPN services under the WTO framework. This in turn requires looking at the relevant commitments in China's GATS Schedule in the sector(s) and mode(s) of delivery affected by the measure.

1. Scheduling Commitments on Digital Services

Under the WTO framework, a member's GATS Schedule contains commitments on market access and national treatment for each sector. These commitments are inscribed as "None" (meaning full commitment), "Unbound" (implying no commitment), or "Limited" i.e. subject to limitations, terms, conditions and qualifications.[98] In addition, a member may inscribe additional commitments including on "qualifications, standards or licensing matters."[99] These Schedules effectively indicate Members' willingness to open up their domestic market to "foreign competition" in different service sectors.[100]

Majority of Members have relied on a note provided by the WTO Secretariat known as Doc. W/120 and the Provisional Central Product Classification (CPC Prov.) in constructing their GATS Schedules.[101] Doc. W/120 contains a classification of the

---

96. This section should be read alongside the Chinese GATS commitments on computer and telecommunications services contained in the Annex.

97. *See* Lucy Hornby, *China's VPN Crackdown is About Money as Much as Censorship*, FIN. TIMES (Jan. 22, 2018), https://www.ft.com/content/35eafc9a-fcf8-11e7-9b32-d7d59aace167.

98. GATS, *supra* note 12, art. XX.

99. GATS, *supra* note 12, at arts. XX.1(c), art. XVIII.

100. Shin-yi Peng, *GATS and the Over-the-Top (OTT) Services—A Legal Outlook*, 50 J. WORLD TRADE 21, 45 (2016).

101. Rousi Zhang, *Covered or Not Covered: That is the Question — Services Classification and its Implications for Specific Commitments Under the GATS*

services economy, dividing the whole economy into 12 service sectors, and was prepared by the GATT Secretariat on the request of the Members in 1991.[102] This document cross-refers each sector to a corresponding heading in the CPC Prov. The Central Product Classification (CPC) is a product-based classification system, first published by the UN in 1991. Additionally, the GATT Secretariat also prepared guidelines for scheduling commitments (Scheduling Guidelines) to provide a concise explanation to Members as to how to achieve precision and clarity in their Schedules.[103] Doc. W/120 and Scheduling Guidelines are important in the context of reading commitments as they encourage a common format and terminology for Members' Schedules, and thus make them comparable across Members.[104]

WTO tribunals have recognized the importance of Doc. W/120 and the Scheduling Guidelines in interpreting Members' Schedules under GATS.[105] In *US – Gambling*, the AB held that the Scheduling Guidelines and Doc. W/120 could be used in interpreting members' Schedules as a "supplementary means of interpretation."[106] As this was a dispute related to the remote supply of gambling services, the AB considered these documents helpful in determining the meaning of "sporting" in the US Schedule and whether this term covered online gambling

---

3 (WTO, Working Paper No. ERSD-2015-11, 2015), https://www.econstor.eu/bitstream/10419/125800/1/845007270.pdf.

102. *See generally* World Trade Organization, *Note by the Secretariat: Services Sectoral Classification List*, WTO Doc. MTN.GNS/W/120 (July 10, 1991) [hereinafter Doc W/120].

103. *See generally* GATT Secretariat, *Scheduling of Initial Commitments in Trade in Services: Explanatory Note*, GATT Doc. MTN.GNS/W/164 (Sept. 3, 1993).

104. *Id*. ¶ 1.

105. Even within the GATT context, the AB in *EC – Computer Equipment* recognized the significance of the Harmonized System (and Explanatory Notes) but did not take a position on their legal value in interpretation of EC's schedule. *See* Appellate Body Report, *European Communities Customs Classification of Certain Computer Equipment*, ¶ 89, WTO Doc. WT/DS62/AB/R (adopted June 22, 1998) [hereinafter EC – Computer Equipment AB Report].

106. *See* Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 196, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005) [hereinafter US – Gambling AB Report] (where the AB held that Scheduling Guidelines and Doc W/120 did not constitute context for interpreting GATS under *Vienna Convention on Law of Treaties* ('VCLT') art. 31 but constitutes supplementary means of interpretation under VCLT art. 32).

services.[107] Previously, in *Mexico – Telecoms*, the Panel recognized the Scheduling Guidelines as "circumstances" pertaining to the conclusion of GATS.[108] However, the Scheduling Guidelines clarify that Members can diverge from Doc. W/120 and create their own classification or definition of sectors or sub-sectors in their Schedules, provided the explanation is "sufficiently detailed" so as "avoid any ambiguity as to the scope of the commitment."[109]

Since the CPC. Prov dates back to 1991, and the Scheduling Guidelines were last revised in 2001, significant confusion exists as to the extent to which Members' Schedules are based on this classification scheme cover modern-day digital services.[110] It can be argued that Members' GATS Schedules must be interpreted in a technologically neutral manner, thus, accounting for evolution of technologies,[111] as discussed in greater detail in the next section.[112] In the absence of any consensus on the classification of several emerging digital services at the WTO, it remains debatable whether a certain digital service has evolved from a pre-existing service as a modification or is an entirely new service outside the ambit of Doc. W/120 and Scheduling Guidelines.[113]

A similar question arises with respect to VPN services. VPNs did not exist at the time when the GATS came into force. As argued in the section below, however, VPN services could be within the scope of telecommunication services as "private leased circuit services." This reading would be consistent with a technologically neutral approach, which has also been endorsed in WTO disputes.[114] China joined the WTO in 1999 and VPN

---

107. *Id.*, ¶ 189–95.

108. This finding was under VCLT art. 32. *See* Panel Report, *Mexico — Measures Affecting Telecommunications Services*, ¶ 7.44, 7.67, WTO Doc. WT/DS204/R (adopted June 1, 2004).

109. *Scheduling of Initial Commitments in Trade in Services*, *supra* note 103, ¶ 16.

110. *See generally* ROLF H. WEBER & MIRA BURRI, CLASSIFICATION OF SERVICES IN THE DIGITAL ECONOMY (2013).

111. L. Lee Tuthill, *Cross-Border Data Flows: What Role for Trade Rules?*, *in* RESEARCH HANDBOOK ON TRADE IN SERVICES 357, –370-71 (Pierre Sauvé & Martin Roy eds., 2016).

112. See text accompanying note 130–33 below.

113. Zhang, *supra* note 101, ¶ 14-16.

114. *See, e.g.*, Appellate Body Report, *China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶ 364, WTO Doc. WT/DS363/AB/R (adopted Jan. 19, 2010) [hereinafter China — Publications and Audiovisual Products AB

services first became available in 1996,[115] thereby, making it harder for China to argue that it had not made any relevant GATS commitments on VPN services.

The next question is the relevant mode of delivery of service under GATS.[116] VPN services can be provided remotely via the internet. Therefore, when foreign suppliers provide VPN services in China, an internet user in China connects to a foreign VPN service for example, it qualifies as a cross-border delivery "from the territory of one Member into the territory of another Member" (also known as Mode 1 delivery).[117] Further, foreign suppliers can also establish their offices in China and provide VPN services via Mode 3 or "by a service supplier of one Member, through commercial presence in the territory of any other Member."[118] Thus, Chinese commitments on both Modes 1 and 3 could be relevant in the context of supply of VPN services to Chinese users.

2. VPN Services: Telecommunications or Computer Services?

VPN services "create a private network via tunneling and/or encryption over the public Internet."[119] Users who want access to such private networks can lease these services from the available providers. These networks provide more secure connections than public networks as they conceal the user's personal information.[120] In order to provide users access to a network, VPN services provide a "comprehensive . . . solution" consisting of "dial-in access," access "to multiple remote sites connected by leased lines (or other dedicated means)," web hosting and supporting intra and inter-VPN connectivity including to the

---

Report]. *See also* Panel Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶ 7.1147, 7.1153, WTO Doc. WT/DS363/R (adopted Jan. 19, 2010) [hereinafter China — Publications and Audiovisual Products Panel Report].

115. Vuk Mujović, *The History of VPN*, LEVPN (Aug. 17, 2018), https://www.le-vpn.com/history-of-vpn/.

116. Four modes of delivery are listed in GATS. *See* GATS, *supra* note 12, at art. I:2.

117. This mode of delivery is also known as Mode 1 Delivery. *See* GATS, *supra* note 12, at art. I:2.

118. *See* GATS, *supra* note 12, at art. I:2.

119. Paul Fergusson & George Huston, *What Is a VPN? — Part I*, *in* THE INTERNET PROTOCOL JOURNAL 1 (1998), https://www.potaroo.net/papers/1998-3-vpn/vpn.pdf.

120. *Id.* at 2.

internet.[121] The question then arises as to the nature of VPN as a service and if VPN services can be classified as per China's GATS Schedule.

At first sight, the relevant sector for VPN services could be telecommunications services, as VPN services connect users to a private network. Alternatively, they could be computer and related services, as VPN services incorporate certain software and webhosting services that enable connecting to a private network through the internet. China has taken the position that all internet access and content services, including VPN services, fall within the scope of telecommunications services.[122] This is unsurprising as China has relatively narrower national treatment and market access commitments at the WTO as compared to computer services.[123]

For instance, in its commitments on market access under Modes 1 and 3 for telecommunications services, both basic and value-added telecommunication services, China has committed to permit foreign companies to establish joint ventures (JVs) with local companies, provided that the foreign equity in such JVs does not exceed 50 percent.[124] In contrast, for computer and related services, China has prescribed broader commitments, such as full commitments on market access in Mode 1 for consultancy, software implementation, data processing (input preparation), data processing and tabulation, and time-sharing services. Further, China has also offered full commitments on market access in Mode 3 for consultancy, data processing and tabulation, and time-sharing services, and also allows fully owned foreign enterprises in software implementation and data processing services.[125]

---

121. *Id.* at 3.

122. *See* U. S. INFO. TECH. OFF., COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION, 2017 WRITTEN COMMENTS TO THE U.S. GOVERNMENT INTERAGENCY TRADE POLICY STAFF COMMITTEE IN RESPONSE TO FEDERAL REGISTER NOTICE REGARDING CHINA'S COMPLIANCE WITH ITS ACCESSION COMMITMENTS TO THE WORLD TRADE ORGANIZATION 14–15 (2017), http://www.bsa.org/~/media/Files/Policy/Trade/09202017USITO2017WTOComplianceFiling.pdf [hereinafter Computing Technology Industry Association].

123. See *Annex.*

124. *See* Council for Trade in Services, *People's Republic of China—Schedule of Specific Commitments*, ¶ 17–18, WTO Doc. GATS/SC/135 (Feb. 14, 2002) [hereinafter Council for Trade in Services].

125. *Id.* at 9–10.

Although certain component services for VPN services are computer services such as webhosting and software services, it could be argued that the VPN service itself is a distinct service that requires tunnelling or encryption over a public telecommunications network. The findings in some WTO disputes are informative in making this assessment. In *China – Electronic Payments*, the Panel held that although electronic payment services could be enabled by a variety of other component services, they were holistically integrated in the delivery of a "new" and "distinct" service, namely, electronic payment service, which the Panel deemed an "integrated service."[126] Similarly, in another WTO dispute, *EC – Bananas III*, the Panel held that the "principal service" ,wholesale trade service, was comprised of subordinate services such as sorting, refrigerating, and delivering goods, which were not "performed as a separate service in their own right."[127]

Further, Doc. W/120 lists "private leased circuit services" under telecommunications services (Heading 2.C) covering CPC 7522 (business network services) which includes dedicated network services (CPC 75222).[128] VPN Services would fall within this category as they are dedicated private networks allowing encrypted access over the public network of the internet. Thus, any software or webhosting service that is necessary to provide VPN connections can be seen as a subordinate service with the VPN itself being the final and distinct telecommunications service.

The next issue is examining the kind of commitments made by China in their GATS Schedule on VPN services. This requires examining the wording of the relevant commitments on telecommunication services in the Chinese Schedule.[129] An examination of the relevant parts of the Chinese Schedule suggests that the most relevant sub-sector for VPN services is "private leased

126. *See* Panel Report, *China—Certain Measures Affecting Electronic Payment Services*, ¶ 7.195, 7.198, WTO Doc. WT/DS413/R (adopted Aug. 31, 2012) [hereinafter *China—Electronic Payment Services Panel Report*].

127. *See* Panel Report, *European Communities—Regime for the Importation, Sale, and Distribution of Bananas*, ¶ 7.291, WTO Doc. WT/DS27/R/ECU (adopted Sept. 25, 1997) [hereinafter *EC—Bananas III Panel Report*].

128. See Annex, C(g) in commitments on telecommunication services stating, 'use of private leased circuit service is permitted' at ¶ 43.

129. *Id.*

circuit services," as explained above. As per VCLT art. 31,[130] the ordinary meaning of the terms of the treaty, including the terms of a Schedule, should be interpreted in good faith by looking at its context and object/purpose.[131] The term private leased circuit services would ordinarily include VPN services offering dedicated networks that can be hired/bought for obtaining private and secure connection to the internet. Further, in *US – Gambling*, the AB held that "context" includes the remainder of the Member's Schedule, the provisions of GATS and other WTO agreements, and the Schedule of other Members.[132] Although the Chinese Schedule does not explicitly refer to CPC Prov. or Doc. W/120, nothing in the Schedule, under telecommunications services or elsewhere, suggests that China intended to adopt any other meaning or deviate from the general understanding of "private leased circuit services" in Doc. W/120 or CPC Prov.

---

130. The customary rules of treaty interpretation are contained in *Vienna Convention on Law of Treaties* ('VCLT') articles 31, 32 and 33, and are frequently relied on by the AB and Panels to clarify the meaning of terms in WTO agreements. *See, e.g.*, Appellate Body Report, *United States—Standards for Reformulated and Conventional Gasoline*, 16–17, WTO Doc. WT/DS2/AB/R (adopted May 20, 1996) [hereinafter *US—Gasoline AB Report*]; Panel Report, *Japan—Taxes on Alcoholic Beverages*, 105, WTO Doc. WT/DS8/R (adopted Nov. 1, 1996); Appellate Body Report*, United States—Import Prohibition of Certain Shrimp and Shrimp Products*, ¶ 114, WTO Doc. WT/DS58/AB/R (adopted Nov. 6, 1998) [hereinafter *US—Shrimp AB Report*]; US – Gambling AB Report, *supra* note 106, ¶ 160; *China—Electronic Payment Services Panel Report*, *supra* note 126, ¶ 7.8; Panel Report, *United States—Measures Affecting The Cross-Border Supply of Gambling and Betting Services*, ¶ 6.45, WTO Doc. WT/DS285/R (adopted Apr. 20, 2005) [hereinafter *US—Gambling Panel Report*]. The Appellate Body has accepted VCLT article 33 as a customary rule. *See* Appellate Body Report, *United States—Final Countervailing Duty Determination with Respect to Certain Softwood Lumber from Canada*, ¶ 59, WTO Doc. WT/DS257/AB/R (adopted Feb. 27, 2004); Appellate Body Report, *Chile—Price Band System and Safeguard Measures Relating To Certain Agricultural Products*, ¶ 271, WTO Doc. WT/DS207/AB/R (adopted Oct. 23, 2002).

131. The AB has held that in interpreting the scope of commitments in members' Schedules in light of VCLT article 31, the 'common intention of the parties' must be found. In deriving the common intention of parties with respect to commitments in a specific Schedule, the unilateral expectation or intention of the Member is irrelevant as relying upon the same undermines security and predictability of the member's Schedules for all other members. *See* EC – Computer Equipment AB Report, *supra* note 105, ¶ 80-–99 (particularly ¶ 84).

132. US – Gambling AB Report, *supra* note 106, ¶ 178. *But see id.*, ¶ 182 (cautioning the use of other members' Schedules as context because of 'intrinsic logic' of individual Schedules.). *See also* China — Publications and Audiovisual Products Panel Report, *supra* note 114, ¶ 7.1182.

Further, WTO law recognizes the principle of technological neutrality, which grants identical legal treatment irrespective of the product's technology. In *China – Publications and Audiovisual Products*, China argued that online music services were a new type of service and, thus, not covered by their commitment on sound recording distribution services, which was limited to distribution in physical medium.[133] China also argued that when making the commitments on sound recording distribution services, digital music distribution services were not available, thus none of the parties intended to make any commitments regarding these services.[134] As per China, these factors constituted relevant circumstances existing at the time of conclusion of the agreement.[135] The AB rejected these arguments, and instead held that whether sound recordings were distributed electronically or on a physical medium was irrelevant.[136] Thus, both distribution of physical and electronic copies of music constituted "sound recording distribution services."[137] Further, in *US – Gambling*, although this issue was not directly in dispute, the Panel referred to the statement of the Work Programme on Electronic Commerce that GATS obligations apply in a technologically neutral manner.[138]

3. Chinese Commitments on VPN Services

In its Schedule with respect to both international and domestic private leased circuit services,[139] China has inscribed commitments with respect to market access under Mode 3 of GATS art. XVI allowing foreign service suppliers to establish joint ventures (JVs) in different areas of China, provided the investment in these JVs does not exceed 49 per cent.[140] With respect to national treatment, China has offered full commitments in Modes 1, 2

133. China — Publications and Audiovisual Products Panel Report, *supra* note 114, ¶ 4.148, 4.149.

134. *Id.*, ¶ 4.155.

135. *Id.*, ¶ 7.1164.

136. China — Publications and Audiovisual Products AB Report, *supra* note 114, ¶ 364. *See also* China — Publications and Audiovisual Products Panel Report, *supra* note 114, ¶ 7.1147, 7.1153.

137. China — Publications and Audiovisual Products AB Report, *supra* note 114, ¶ 364.

138. *See also US—Gambling Panel Report*, *supra* note 130, ¶ 6.285.

139. *See* Annex, C(g) in commitments on telecommunication services stating, 'use of private leased circuit service is permitted' at 43.

140. *See* Council for Trade in Services, *supra* note 124, at 20.

and 3 on domestic and international private leased circuit services.[141]

GATS art. XX:2 requires that if a member intends to impose restrictions in a sector that are inconsistent with obligations on national treatment and market access, the restrictions must only be inscribed in the column on market access in the Member's Schedule. This inscription will "be considered to provide a condition or qualification to Article XVII as well."[142] Thus, the inscription in GATS art. XVII with respect to national treatment should be interpreted harmoniously with the limitations prescribed in GATS art. XVI on market access. In other words, a discriminatory measure that is inconsistent with national treatment obligations does not violate GATS if that measure is covered by the inscriptions on market access.[143] Under GATS art. XX:2, since China has inscribed full commitments on national treatment, it cannot discriminate against foreign suppliers of VPN services.[144] But the participation of foreign suppliers in the domestic market is contingent on them satisfying the two conditions of market access: (i) the foreign supplier forms a joint venture with a local company; and (ii) the foreign company's share does not exceed 49 percent.

Conclusively, China has offered relevant market access commitments on VPN services that allow foreign suppliers to offer VPN services in China provided they form JVs with local companies, with foreign equity in these JVs not exceeding 49 percent. Further, since China has inscribed full commitments on national treatment, it cannot discriminate against foreign suppliers of VPN services, provided they meet the conditions of market access by forming a JV with a local company with foreign equity not exceeding 49 percent.

---

141. *Id*.

142. GATS, *supra* note 12, at art. XX:2. *See also China—Electronic Payment Services Panel Report*, *supra* note 126, ¶ 7.656.

143. *See, e.g.*, *China—Electronic Payment Services Panel Report*, *supra* note 126, ¶ 7.663–7.664.

144. Art. XX:2 requires that measures inconsistent with both art XVI and art XVII shall be inscribed in the column relating to art XVI.

D. Consistency of Chinese VPN Measure with GATS Obligations

1. Market Access

The obligation on market access is contained in GATS art. XVI. This provision prohibits Members from adopting or maintaining measures in sectors where they have made commitments limiting the "number of service suppliers," "total value of service transactions or assets," "total number of service operations or on the total quantity of service output," "total number of natural persons that may be employed in a particular service sector or that a service supplier may employ," "the participation of foreign capital," and "restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service."[145] GATS art. XVI has a significant effect on "market contestability" as it is aimed at creating a level playing field between foreign and domestic services and service suppliers.[146]

The Chinese Schedule requires all foreign VPN suppliers to establish JVs with local partners, with foreign equity not exceeding 49 percent, as a condition of accessing the domestic markets. In *US – Gambling*, the AB held that even if a member makes commitments on market access for a specific sector, it is not prohibited from imposing reasonable regulations for licensing or authorizing supply of such services in the domestic market.[147]

At face value, the Chinese VPN measure does not appear to be a violation of market access (GATS art. XVI) because any foreign service supplier (i.e., those that have formed JVs as per the legal requirements) can apply for a license from the Chinese telecommunications regulator to supply VPN services in China for cross-border network connections. Despite strict regulations on international VPN connections in China due to their classification as BTS, foreign service providers can still apply for a license through the MIIT to offer cross-border network connections, though requirements may be difficult to meet.[148] Further, the BT

145. GATS, *supra* note 12, at art. XVI: 2.

146. Gilles Muller, *Troubled Relationships under the GATS: Tensions between Market Access (Article XVI), National Treatment (Article XVII), and Domestic Regulation (Article VI)*, 16 WORLD TRADE REV. 449, 450 (2017).

147. US – Gambling AB Report, *supra* note 106, ¶ 25–26.

148. Tania Voon & Andrew Mitchell, *Open for Business? China's Telecommunications Service Market and the WTO*, 13 J. INT'L ECON. L. 321, 367 (2010)

Group, a British telecommunications company, has successfully obtained a license from the MIIT to provide domestic network VPN services by establishing a JV with a Chinese company.[149] Thus, it may be hard to argue that the Chinese VPN measure prohibits the supply of foreign VPN services in China inconsistent with China's market access obligations under GATS art. XVI.[150]

2. National Treatment

Any measure affecting trade in services violates the national treatment obligation in GATS art. XVII if it fails to accord foreign services and service suppliers "treatment no less favorable than that it accords to its own like services and service suppliers."[151] Being a specific obligation, it applies only in those sectors where Members have offered commitments in their GATS Schedule of Commitments.[152] An example of a national treatment violation is a ban on foreign service suppliers to provide online content or social networking sites while permitting similar services by domestic companies.

Applying the national treatment obligation (GATS art. XVII) to the Chinese VPN measure entails determining: (i) the likeness of domestic and foreign VPN services or service suppliers; and (ii) whether foreign VPN service(s) or service supplier(s) have received less favorable treatment compared to domestic VPN service(s) or service supplier(s). The commitments on national treatment in China's Schedule should be read in light of the inscriptions in GATS art. XVI, i.e., a foreign supplier of VPN services can form a JV with a local partner and its share must not exceed 49 percent. Thus, this section examines whether: (i)

(explaining that international VPN connections are classified as BTS, which is more stringently regulated in China).

149. Press Release, BT, First Global Telco to Receive Domestic Telecoms Licenses in China, (Jan. 24, 2019), https://www.globalservices.bt.com/en/aboutus/news-press/bt-first-global-telco-to-receive-domestic-telecoms-licences-in-china.

150. Voon & Mitchell, *supra* note 148, at 355.

151. GATS, *supra* note 12, at art. XVII:1.

152. A measure violating market access obligations (*see* GATS art. XVI) may also fall under GATS art. XVII. GATS, *supra* note 12, at art. XVII;. *see China—Electronic Payment Services Panel Report*, *supra* note 126, at ¶ 7.649–7.664 (the panel decided that if commitments are inscribed in both GATS art. XVI and XVII, the inscriptions under GATS art. XVI prevails)*; see also* GATS, *supra* note 12, at art. XX:2.

foreign and domestic VPN services and service suppliers are like; (ii) whether foreign VPN services or service suppliers applying to operate as a JV in China receive less favorable treatment compared to domestic VPN services or service suppliers.

Under GATS art. XVII, the first step is assessing whether foreign and domestic VPN services and service suppliers are "like." When a measure differentiates domestic and foreign services/service suppliers exclusively based on the country of origin (or a de jure discrimination), 'likeness' can be presumed.[153] The AB, however, has noted that presuming likeness of services or service suppliers is "more limited" than presuming likeness of goods and depends on "the nature, configuration, and operation of the measure at issue and the particular claims raised."[154] Here, the Chinese VPN measure does not prevent foreign suppliers from applying for a license to supply international VPN services in China, provided they meet the conditions of market access, discussed in the previous section. This measure does not differentiate between foreign and domestic VPN services or service suppliers based on their origin, because any unlicensed VPN service, domestic or foreign, is prohibited to be supplied in China. Hence, likeness of foreign and domestic VPN services or service suppliers cannot be presumed.

In the absence of de jure discrimination, foreign and domestic services and service suppliers can be considered "like" under GATS art. XVII if a "competitive relationship" exists between foreign and domestic services/service suppliers.[155] The likeness of goods is examined under GATT considering: (i) properties, nature, and quality of goods; (ii) end-uses; (iii) consumers' tastes and habits or perceptions and behavior; and (iv) tariff classification of goods.[156] In *Argentina – Financial Services*, the AB held

153. Argentina – Financial Services AB Report, *supra* note 90, ¶ 6.38.

154. *Id.* ¶ 6.41.

155. *See, e.g.*, *China—Electronic Payment Services Panel Report*, *supra* note 126, ¶ 7.700; Panel Report, *Argentina—Measures Relating to Trade in Goods and Services*, ¶ 7.170–71.73, WTO Doc. WT/DS453/R (adopted May 9, 2016); Argentina – Financial Services AB Report, *supra* note 90, ¶ 6.22, 6.24. Art. XVII:3 GATS states that "different treatment shall be considered to be less able if it modifies the conditions of competition." *See* GATS, *supra* note 12, at art. XVII:3.

156. Appellate Body Report, *European Communities—Measures Affecting Asbestos And Asbestos-Containing Products*, ¶ 102, WTO Doc., WT/DS135/AB/R (adopted Mar. 12, 2001) [hereinafter *EC—Asbestos AB Report*]; *see also*

that the above factors are also relevant for GATS, provided that they are "adapted as appropriate to account for the specific characteristics of trade in services."[157] Thus, in the context of GATS, the pertinent factors in examining competition between different services are the intrinsic character or nature, including quality of the services, their end use, consumer perceptions, and the relevant classification under Doc. W/120.[158]

Applying the above criteria, foreign and domestic VPN services and service suppliers can be considered "like" for the following reasons. First, the basic function of any VPN service is ensuring secure connection to a private network to access content available over the public internet. As such, no evidence exists that the quality or technology of foreign VPN services is materially different from domestic Chinese services, except that the latter are mostly supplied by state-owned enterprises.[159] Second, both foreign and domestic VPN services are used for the purposes of bypassing the firewall of the Chinese government that blocks several websites and applications and hence their end-uses are similar. Third, people seeking to communicate or access information via VPN services do not necessarily distinguish between foreign and domestic services; rather, as the Chinese government regulates this sector very stringently, internet users are forced to use whatever services are available.[160] Moreover, as state-owned enterprises offer more expensive VPN services with arguably lower levels of privacy and security,[161] most

---

Working Party on Border Tax Adjustment, *Secretariat Note on Meeting of 30 April to 2 May 1968*, ¶ 18, WTO Doc. L/3009 (May 17, 1968).

157. Argentina – Financial Services AB Report, *supra* note 90, ¶ 6.30–32. *See also EC—Bananas III Panel Report*, *supra* note 127, ¶ 7.322. *But see China—Electronic Payment Services Panel Report*, *supra* note 126, ¶ 7.698 ("[W]e do not assume that without further analysis we may simply transpose to trade in services the criteria or analytical framework used to determine 'likeness' in the context of the multilateral agreements on trade in goods. We recognize important dissimilarities between the two areas of trade.").

158. *See* Argentina – Financial Services AB Report, *supra* note 90, ¶ 6.30; *see also* NICOLAS F. DIEBOLD, NON-DISCRIMINATION IN INTERNATIONAL TRADE IN SERVICES: 'LIKENESS' IN WTO/GATS 245–67, 353 (2010).

159. The fact that a majority of Chinese suppliers are state-owned, while foreign ones are not, is irrelevant in this case as both of them provide VPN services. *See EC—Bananas III Panel Report*, *supra* note 127, ¶ 7.322.

160. Hornby, *supra* note 97.

161. Brian Fung, *Here's China's Latest Plan to Keep its Citizens from the Open Internet*, WASH. POST (July 10, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/07/10/heres-chinas-latest-plan-to-keep-

Chinese internet users are likely to prefer foreign VPN services, if available. Finally, domestic and foreign VPN services fall under the same heading in Doc. W/120, as explained earlier. Thus, it can be concluded that foreign and domestic VPN services are competitors in the same market and therefore should be considered "like" under GATS art. XVII.

Next, a measure is said to accord "less favourable treatment" under GATS art. XVII if it "modifies the conditions of competition in favour of services or service suppliers of the Member compared to like services or service suppliers of any other Member."[162] Still, "any inherent competitive disadvantages which result from the foreign character of the relevant services or service suppliers" are excluded from the scope of "less favourable treatment."[163] Thus, GATS art. XVII examines if the measure results in differential treatment by considering how it affects competitive conditions for foreign services and service suppliers, either by discriminating against them, by favoring domestic services and service suppliers, or both.

The Chinese VPN measure appears to skew the competition both directly and indirectly in the domestic market in favor of domestic VPN services and service suppliers and, thus, accords less favorable treatment to foreign VPN services and service suppliers in violation of GATS art. XVII. Several foreign companies have argued that the process of obtaining MIIT's approval for VPN services is much easier for domestic companies.[164] As discussed earlier, according to the Catalogue of Telecom Services by Category issued by the MIIT in 2015, domestic VPN services are categorized as VATS while cross-border VPN services are categorized as BTS.[165] This distinction can significantly increase costs and compliance requirements for any foreign company desiring to provide cross-border network connections as BTS suppliers are required to follow several additional requirements.[166] For example, the capitalization requirement, the company's total value, for BTS is 100 times higher than value-added

---

its-citizens-from-the-open-internet/?noredirect=on&utm_term=.8afd74cdb57e.

162. GATS, *supra* note 12, at art. XVII:3.

163. GATS, *supra* note 12, at art. XVII:1, n. 10.

164. *See* Computing Technology Industry Association, *supra* note 122, at 15.

165. *Id*.

166. *Id*., at 15–16. *See also* Voon & Mitchell, *supra* note 148, at 350–51, 366–67.

telecommunications services.[167] This would prevent foreign VPN service suppliers from entering the Chinese market, especially if they are smaller companies without significant financial resources and, thus, constitutes "less favourable treatment" of foreign services and service suppliers.

3. Domestic Regulation

The Chinese VPN measure can also be examined for consistency with obligations on domestic regulation in GATS art. VI:1, which requires trade measures impacting services to be administered in a reasonable, objective, and impartial manner by each member in sectors with specific commitments.

Further, GATS art. VI:2 and art VI:3 contain general obligations requiring Members to institute tribunals and proper procedures for reviewing and providing remedies for administrative decisions and providing information to applicants regarding approvals related to supplying services.

China has committed to permit foreign companies to supply VPN services in China. However, as per the Chinese VPN measure, all VPN service suppliers must obtain a license from the Chinese telecommunications regulator to supply VPN licenses. This measure can be considered a "measure of general application" as it applies to all service suppliers.[168] Under GATS art. VI, China would therefore be obliged to administer the Chinese VPN measure in a reasonable, objective, and impartial manner. Not enough information is publicly available to conduct the above assessment in a detailed manner. For example, China has not provided any public information regarding the criteria for

---

167. Computing Technology Industry Association, *supra* note 122, at 16.

168. For an explanation of GATT art. X.1's meaning of "measures of general application," *see, e.g.*, Appellate Body Report*, United States—Restrictions on Imports of Cotton and Man-made Fibre Underwear*, 21, WTO Doc. WT/DS24/AB/R (adopted Feb. 25, 1997); Panel Report, *United States—Restrictions On Imports Of Cotton And Man-Made Fibre Underwear*, ¶ 7.65, WTO Doc. WT/DS24/R (adopted Feb. 25, 1997); Panel Report, *European Communities—Selected Customs Matters*, ¶ 7.116, WTO Doc. WT/DS315/AB/R (adopted Dec. 11, 2006); Panel Report, *China—Measures Related to the Exportation of Various Raw Materials*, ¶ 7.772, 7.804, 7.1098, WTO Doc. WT/DS394/R, WT/DS395/R, WT/DS398/R (adopted Feb. 22, 2012) [hereinafter *China—Raw Materials Panel Report*].

investigation of an application by a foreign VPN supplier intending to enter the Chinese market.[169]

Based on information available from press and industry reports, however, it appears that the Chinese VPN measure could violate GATS art. VI:1 in several ways. First, no independent agency or tribunal exists in China to address grievances of foreign VPN suppliers; nor are suppliers notified of changes in Chinese government policy on VPN services.[170] Press reports also indicate that the majority of legal VPN services available in China are supplied by state-owned telecommunication companies and it is generally very difficult for foreign suppliers to obtain licenses for supplying VPN services in China.[171] As discussed in the previous section, the licensing requirements for foreign VPN service providers providing cross-border VPN services is significantly onerous as compared to domestic VPN service providers due to differential classification.[172]

Second, based on press reports, it appears that VPN services in China are blocked by the MIIT in an inconsistent manner without adequate administrative guidelines or procedures.[173] If a complainant is able to adduce evidence of arbitrary discrimination against foreign VPN services or service suppliers in a WTO dispute, the Panel could potentially find a breach of GATS art. VI:1. In past disputes, the AB has criticized the lack of proper guidelines in domestic regulations because it leads to administrative indiscretion and inconsistent application of regulations.[174] Scholars have also highlighted the importance of GATS art. VI:1 in promoting impartiality and consistency in the

169. Based on this, the transparency of the Chinese VPN measure can possibly be examined under GATS art. III. This argument is not explored further due to insufficient available information.

170. *See, e.g.*, Communication from the United States, *Measures Adopted and Under Development by China Relating to its Cybersecurity Law*, ¶ 7, WTO Doc. S/C/W/376 (Feb. 23, 2018). This could be a violation of GATS art. VI:2(a).

171. *Foreign Companies in China Brace for VPN Crackdown*, BUS. TIMES (Mar. 30, 2018, 12:30 PM), https://www.businesstimes.com.sg/government-economy/foreign-companies-in-china-brace-for-vpn-crackdown;
BT Becomes First Foreign Telecoms Firm to Secure Chinese License, CHINESE DAILY (Jan. 29, 2019, 10:44 AM), http://www.chinadaily.com.cn/a/201901/29/WS5c4fbdfca3106c65c34e70b2.html.

172. *See* sec. IIA.

173. Charles Clover, *China Intensifies VPN Services Crackdown*, FIN. TIMES (Jan. 23, 2015), https://www.ft.com/content/46ad9e26-a2b9-11e4-9630-00144feab7de.

174. *China—Raw Materials Panel Report*, *supra* note 168, ¶ 7.744–.746.

administration of domestic regulations, such as approval of licensing applications.[175] For instance, Voon and Mitchell have argued that the MIIT may not meet the independence and impartiality requirement set out in the Reference Paper on Telecommunications (applicable to BTS),[176] which China has incorporated into its GATS Schedule.[177] Section 5 of the Reference Paper sets out that a regulatory body should be independent and impartial, implementing procedures to ensure fairness among all market participants.[178]

Currently, international VPN services are provided in China only by state-owned telecommunications companies (China Telecom, China Unicom and China Mobile), which arguably have a close connection with the government.[179] While China has argued that the MIIT operates as an independent regulator, it remains possible for a panel to infer from available evidence that the lack of any foreign VPN service providers for cross-border network connections could be the result of arbitrary and partial implementation of the licensing requirements rather than based on an objective or reasonable criteria. Such an assessment is expectedly contingent on the evidence that will be brought forth before a panel in a real dispute, especially in the absence of sufficient publicly available information, but it remains possible to argue that the Chinese VPN measure could violate various obligations contained in GATS art. VI.

4. GATS Telecommunications Annex

China is bound by the obligations listed in GATS Annex on Telecommunication Services, which applies to "measures affecting access to and use of public telecommunications transport networks and services."[180] This Annex should be read along with the individual commitments offered by China on telecommunications services.[181]

---

175. Shin-yi Peng, *The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?*, 22 J. INT'L ECON. L. 1, 27 (2019).

176. *Negotiating Group on Basic Telecommunications*, WTO (Apr. 24, 1996), https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

177. Voon & Mitchell, *supra* note 148, at 333–34.

178. WTO, *supra* note 176.

179. Voon & Mitchell, *supra* note 148, at 333–34.

180. GATS, *supra* note 12, at Annex on Telecommunications ¶ 1.

181. *Id.* at ¶ 2(c)(i).

Certain Members have argued that the Chinese VPN measure is inconsistent with Para 5(c) of GATS Telecoms Annex:

> Each Member shall ensure that service suppliers of any other Member may use public telecommunications transport networks and services for the movement of information within and across borders, including for intra-corporate communications of such service suppliers, and for access to information contained in data bases or otherwise stored in machine-readable form in the territory of any Member. Any new or amended measures of a Member significantly affecting such use shall be notified and shall be subject to consultation, in accordance with relevant provisions of the Agreement. [182]

The Chinese VPN measure restricts corporate communications between foreign companies operating in China and their overseas headquarters by preventing unhindered access to foreign servers, and thus, the only option for foreign companies is to access international VPN services provided by Chinese telecommunications operators.[183] As authorized VPN services in China are largely limited to state-owned enterprises subject to more extensive government surveillance,[184] the Chinese VPN measure is likely to compromise the confidentiality and security of intra-corporate communications. Further, foreign companies could be concerned about possible cyber espionage occurring through the VPN networks provided by state-owned companies.

Although China notified this measure in February 2017, it has yet to conduct a public consultation allowing affected parties to make representations, which could potentially be a breach of the requirement under GATS art. 5(c).[185]

Further, the Annex contains provisions that directly apply to private leased circuit services (which, as explained earlier, includes VPN services).

Each Member shall ensure that service suppliers of any other Member have access to and use of any public telecommunications transport network or service offered within or across the border of that Member, including private leased circuits, and to this end shall ensure, subject to paragraphs (e) and (f), that such suppliers are permitted:

---

182. *See, e.g.*, *Measures Adopted and Under Development by China Relating to its Cybersecurity Law*, *supra* note 170, ¶ 7.

183. Chinese VPN Measure, *supra* note 13.

184. Houweling, *supra* note 80.

185. *See, e.g.*, *id*.

> (ii) to interconnect private leased or owned circuits with public telecommunications transport networks and services or with circuits leased or owned by another service supplier;[186]

The above provision is subject to art. 5(e), which allows Members to impose conditions "necessary [to] safeguard the public service responsibilities of suppliers of public telecommunications transport networks and services."[187] "Public service responsibility" is a vague term that can be interpreted to include removal of access to unauthorized or illegal VPN services. This provision has not been tested in a WTO dispute; however, the presence of the term "necessary" in art. 5(e) suggests that there needs to be a determination regarding the necessity of the measure. For example, there needs to be an inquiry into whether the Chinese VPN measure is necessary to remove illegal activities on the internet (this assessment is continued in the next section). If the Chinese VPN measure is considered necessary under art. 5(e), China can impose restrictions on the "inter-connection of private leased or owned circuits . . . or with circuits leased or owned by another service supplier," without violating the GATS Telecommunications Annex.[188]

E. Justifying the Chinese VPN Measure under the GATS Art. XIV Exception

The previous section argued that the Chinese VPN measure is likely to be inconsistent with GATS art. XVII, art. VI and, possibly, art. 5(c) and (b)(ii) of GATS Telecommunications Annex. However, measures inconsistent with GATS obligations may fall under the GATS exceptions, such as GATS art. XIV. This section assesses the necessity of the Chinese measure to fulfil GATS art. XIV policy objectives and comply with GATS art. XIV chapeau. The analysis involves two steps: (i) identifying if the measure falls under any exceptions listed in GATS art. XIV, provisionally justifying it, and (ii) verifying if it meets the terms of GATS art. XIV chapeau.[189]

A "fine line" exists between legitimate measures implemented to achieve legitimate social policies with incidental negative trade effects, and measures that disguise an outright abuse of

186. GATS, *supra* note 12, at Annex on Telecommunications ¶ 5(b)(ii).
187. *Id.* at ¶ 5(e)(i).
188. *Id.* at ¶ 5(f)(v).
189. *US—Gasoline AB Report*, *supra* note 130, at 22.

WTO obligations as being necessary for social policy objectives.[190] The assessment below in the context of the Chinese VPN measure highlights the various challenges involved in treading this fine line.

1. Relevance of GATS Exceptions

The Chinese VPN measure is purportedly aimed at reducing illegal activities in Chinese cyberspace and promoting an orderly and healthy development of the internet industry. Companies and individual users in China mainly use VPN services to access banned foreign websites or applications.[191] Accordingly, one of the purposes behind the measure is censoring online content to maintain consistency with domestic values, including maintaining the stability of the political order and enforcing specific sociocultural norms. Another stated rationale of the measure is strengthening the management of cybersecurity issues.[192] The latter rationale is perhaps less convincing. For example, the requirements to create a centralized user archive and to limit communication via VPNs to business purposes do not strengthen cybersecurity. Rather, these requirements end up restricting access to banned websites and applications in China. Nonetheless, China could rely on either of these policy rationales to justify the measure under GATS art. XIV(a) and art. XIV(c).

GATS art. XIV(a) allows Members to impose any measures that are necessary to protect public morals or maintain public order. GATS art. XIV(a) further states that the "public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society."[193] GATS art. XIV(c) allows Members to impose any measures "necessary to secure compliance with laws or regulations" which are not otherwise inconsistent with WTO law, including, but not limited to, laws aimed at preventing "deceptive and fraudulent practices" relating to the "effects of a default on services contracts,' 'protection of privacy of individuals," "protecting confidentiality of individual records and accounts" and "safety."[194]

190. SIMON LESTER, BRYAN MERCURIO & ARWEL DAVIES, WORLD TRADE LAW 374 (3d ed. 2018).

191. *See* Wei, *supra* note 74.

192. Chinese VPN Measure, *supra* note 13, at pmbl.

193. GATS, *supra* note 12, art. XIV(a), n. 5.

194. GATS, *supra* note 12, art. XIV(c).

Let us start with the relevance of GATS art. XIV(a) to the Chinese VPN measure. The term "public morals" is not defined in GATS, however, it has been interpreted very liberally in WTO disputes, without second-guessing the stated policy objectives of the defendant.[195] In an oft-quoted phrase from *US – Gambling*, the Panel held that "'public morals' denotes standards of right and wrong conduct maintained by or on behalf of a community or nation."[196] Further, the Panel held that public morality was context-specific and could vary from member to member depending on their "prevailing social, cultural, ethical and religious values."[197] The AB in *EC – Seals*[198] and the Panel in *China – Publications and Audiovisual Products*[199] took a similar approach in defining "public morals." In *Brazil - Taxes and Charges*, the Panel even accepted Brazil's argument that bridging the digital divide and promoting social inclusion sufficiently qualified as protecting public morals.[200] A recent Panel decision in the US – *Tariff Measures* also took a similarly broad approach in defining the scope of public morals.[201]

By restricting unauthorized VPN services and imposing strict requirements for the use of authorized VPN services,[202] the Chinese VPN measure is likely to reduce access to politically offensive content, such as criticism of the ruling party in China, discussions of controversial political ideologies,[203] and sensitive

195. Ming Du, *How to Define 'Public Morals' in WTO Law? A Critique of Brazil – Taxation and Charges Panel Report*, 13 GLOB. TRADE & CUSTOMS J. 69, 72–74 (2018).

196. *US—Gambling Panel Report*, *supra* note 130, ¶ 6.465.

197. *Id.*, 6.461.

198. Appellate Body Report, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products*, ¶ 5.199, WTO Doc. WT/DS400/AB/R (adopted June 18, 2014) [hereinafter *EC – Seal Product AB Report*].

199. China — Publications and Audiovisual Products Panel Report, *supra* note 114, ¶ 7.759.

200. Panel Report, *Brazil – Certain Measures Concerning Taxation and Charges*, ¶ 7.561–7.568, WTO Doc. WT/DS472/R (adopted Jan. 11, 2019) (this finding was not addressed in the Appellate Body Report).

201. *See* Panel Report, *United States – Tariff Measures on Certain Goods from China,* ¶ 7.135–7.139, WTO Doc. WT/DS543/R (Sept. 15, 2020).

202. *See* section IIA.

203. FREEDOM HOUSE, FREEDOM ON THE NET REPORT: CHINA (2018), https://freedomhouse.org/report/freedom-net/2018/china.

socio-cultural content that may harm social or moral order.[204] Further, by requiring a centralized user archive, the Chinese government could track activities of political dissidents. Thus, the Chinese VPN measure acts as a tool to prevent activities that the government considers a threat to the stability of the political and social system.

The next question is whether the Chinese VPN measure is indeed aimed at protecting public morals or maintaining public order in any manner. A question that may arise in this regard is whether the policy objective of the measure (namely controlling the circulation of politically and socially sensitive content) reflects the values of Chinese society at large or if it merely reflects the ethos and/or interests of the ruling party. This question would entail investigating delicate questions, such as whether Chinese citizens agree with the government's censorship policies,[205] and if Chinese censorship laws comply with international human rights norms. Investigating the rationale behind the Chinese VPN measure in such a manner, however, would directly interfere with China's sovereignty.[206] For instance, the Panel might need to investigate the list of websites and applications that are blocked in China for content sensitivity, and whether such content would interfere with protecting public morals or maintaining public order. In addition to being politically sensitive, such an investigation would lack practical feasibility for an international forum with limited domestic enforcement capacity.

In fact, potential complainants may be reluctant to raise their concerns as it may open a can of worms. In a previous dispute at the WTO (*China – Publications and Audiovisual Products*), for example, the US (which has consistently criticized Chinese

204. *See, e.g.*, Jìsuànjī xìnxī wǎngluò hé hùliánwǎng ānquán bǎohù guǎnlǐ tiáolì (計算機信息網絡和互聯網安全保護管理條例)[Computer Information Network and Internet Security, Protection, and Management Regulations] (promulgated by the Ministry of Public Security, Dec. 30, 1997, effective Dec. 30, 1997), arts. 4–6, http://www.asianlii.org/cn/legis/cen/laws/cinaispamr904/ (China) [hereinafter Computer Information Network and Internet Security, Protection and Management Regulations].

205. Panel Report, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products*, ¶ 7.404, WTO Doc. WT/DS400/R (adopted June 18, 2014). *See generally* Qinghua Yang & Yu Liu, *What's on the Other Side of the Great Firewall? Chinese Web users' Motivations for Bypassing the Internet Censorship*, 37 COMPUT. IN HUM. BEHAV. 249, 254–56 (2014) (discussing why Chinese users bypass the Great Firewall of China).

206. *See* Wyatt, *supra* note 50, at 444.

online content regulations) focused its complaint on the discriminatory aspects of China's regulation of online publications and audiovisual services rather than question whether such regulations would qualify under the "public morals" or "public order" defense under GATS art. XIV(a).

Some scholars have taken the view that China's regulations on online content may not satisfy the threshold requirements under GATS art. XIV(a) as it is disproportionate to the objective of safeguarding public morals and/or not directly related to the public morals defense.[207] For instance, Gao argues that "public morals" is relevant to "standards of right and wrong conduct maintained by or on behalf of a community or nation."[208] Since the reference is to "community or nation" rather than the ruling government, the GATS art. XIV(a) exception does not justify any measures prohibiting circulation of online content that the ruling party considers to be sensitive or offensive.[209] In that regard, it is irrelevant under GATS art. XIV(a) whether such content is considered illegal under domestic law (although this could be relevant under GATS art. XIV(c), as discussed below) so long as it reflects the values of the community or nation.[210] Further, the Chinese constitution provides for various rights, such as the freedom of speech and expression, and the freedom of religious belief, which allow individuals to express their unfavorable opinions regarding the ruling party. Accordingly, the public order exception under GATS art. XIV(a) is also irrelevant because accessing information that the ruling party deems sensitive or offensive poses no genuine or fundamental threat to the interests of the society.[211]

As noted earlier, however, the above approach can open a can of worms. First, the extent to which the Chinese constitution guarantees certain rights such as freedom of expression is a matter of domestic sovereignty and, thus, a panel should remain extremely cautious in making any assessment in that regard.

---

207. *See, e.g.*, Zhen, *supra* note 34, at 759.

208. Henry S. Gao, *Google's China Problem: A Case Study on Trade, Technology and Human Rights under the GATS*, 6 ASIAN J. WTO & INT'L HEALTH L. & POL'Y 347, 376 (2011).

209. Claire Wright**,** *Censoring the Censors in the WTO: Reconciling the Communitarian and Human Rights Theories of International Law*, 3 J. INT'L MEDIA & ENT. L. 17 (2010).

210. Gao, *supra* note 208, at 375-6.

211. Gao, *supra* note 208, at 377.

Further, a member advancing a complaint regarding the Chinese VPN measure would be predominantly concerned with their economic interests, and thus, it may appear disingenuous to argue that the Chinese VPN measure frustrates the rights of Chinese people, especially before a trade body such as the WTO. Second, it may be inappropriate for a panel dealing with trade issues to evaluate whether a particular measure reflects the values of the community or a nation, especially when there can be diverse views within the community, even if certain views may have been a result of persistent internet censorship.[212] Finally, as argued below, China may also resort to a defense under GATS art. XIV(c).

GATS art. XIV(c) would be relevant if China could demonstrate that the VPN measure is necessary to achieve compliance with specific domestic laws and regulations that are otherwise consistent with WTO law. To avail under GATS art. XIV(c) exception, a member must show that: (i) there are laws and regulations consistent with GATS; (ii) the measure that breached GATS was designed to comply with these laws and regulations; and (iii) the measure is necessary to secure such compliance.[213] One of the stated policy objectives of the Chinese VPN measure is better management of cybersecurity-related issues.[214] Some experts argue that the security objective behind the Chinese VPN measure is not entirely misplaced. For instance, by restricting the access of users in China to authorized VPN services for cross-border network connections, the Chinese government can better control malicious actors engaged in cyber-crimes or cyber-threats, especially in untrusted encryption networks.[215]

The Chinese VPN measure, as argued earlier, is consistent with and intended to further the objectives set out in previous regulations governing VPNs.[216] Further, China may be able to

---

212. Yaqiu Wang, *In China, the 'Great Firewall' Is Changing a Generation*, HUM. RTS. WATCH (Sept. 1, 2020, 11:57 AM), https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation.

213. US – Gambling AB Report, *supra* note 106, ¶ 339-344.

214. Chinese VPN Measure, *supra* note 13.

215. Anthony Rutkowski, *U.S. Complaint to WTO on China VPNs Is Itself Troubling*, CIRCLEID (Mar. 6, 2018), https://circleid.com/posts/11145/12098/.

216. *See, e.g.*, Guójì tōngxìn chūrùkǒu jú guǎnlǐ bànfǎ (国际通信出入口局管理办法) [Measures for the Administration of International Communications Gateway Exchange Procedures] (promulgated by the Ministry of Industry and Information Technology, June 26, 2002, effective Oct. 1, 2002)

argue that the Chinese VPN measure is essential to achieve compliance with the objectives of its Cybersecurity Law of "ensur[ing] cybersecurity; safeguard[ing] cyberspace sovereignty and national security, and social and public interests; protect[ing] the lawful rights and interests of citizens, legal persons, and other organizations; and promot[ing] the healthy development of the informatization of the economy and society."[217] China could also argue that the VPN measure helps in achieving compliance with various domestic censorship laws.[218] Under GATS art. XIV(c), domestic laws of a member are presumed to be consistent unless shown otherwise.[219] Although it is outside the scope of this Article to discuss the provisions in Chinese cybersecurity laws in detail, it can be presumed that the overall objective is consistent with WTO law (e.g., ensuring cybersecurity of networks or regulating circulation of blasphemous or immoral content).The Panel is likely to look at these laws at face value.

Further, even if certain aspects of a domestic law are inconsistent with WTO law (e.g., a party may challenge the data localization requirement in the Cybersecurity Law),[220] the entire law is not invalidated on account of a WTO challenge. Still, China may need to clearly identify the specific laws and regulations that the Chinese VPN measure seeks to comply with, although it need not demonstrate such compliance with "absolute certainty."[221] As insufficient information is publicly available regarding the administration of the Chinese VPN measure and

---

http://www.zhongguotongcuhui.org.cn/stzl_37497/flfg/bmgzgfxwj/201210/t20121031_3256023.html?_x_tr_sch=http&_x_tr_sl=zh-CN& (China).

217. Rogier Creemers, Paul Triolo, & Graham Webster, *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, NEW AM. (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

218. *See, e.g.*, Computer Information Network and Internet Security, Protection and Management Regulations, *supra* note 204, at arts. 4–6.

219. Appellate Body Report, *United States – Countervailing Measures on Certain Hot-Rolled Carbon Steel Flat Products from India*, ¶ 4.446, WTO Doc. WT/DS436/AB/R (adopted Dec. 19, 2014).

220. Chris Mirasola, *U.S. Criticism of China's Cybersecurity Law and the Nexus of Data Privacy and Trade Law*, LAWFARE (Oct. 10, 2017, 12:00 PM), https://www.lawfareblog.com/us-criticism-chinas-cybersecurity-law-and-nexus-data-privacy-and-trade-law.

221. Appellate Body Report, *India – Certain Measures Relating to Solar Cells and Solar Modules*, ¶ 5.108, WTO Doc. WT/DS456/AB/R (adopted Oct. 14, 2016).

other related laws and regulations, it is not possible to conclusively state if GATS art. XIV(c) will be applicable. Nonetheless, given that the Chinese VPN measure has an underlying security as well as censorship rationale and is prescribed in various domestic laws, GATS art. XIV(c) remains a possible avenue for justifying this measure.

2. The Necessity of the Chinese VPN Measure under GATS art. XIV

WTO tribunals have developed an elaborate necessity test to examine whether a measure is indispensable to achieve a policy objective, including: (i) assessing the relative importance of the interests and values underlying the measure; (ii) "weighing and balancing," in light of those interests and values, the contribution of the measure to the objective, and the restrictive impact of the measure on international commerce; and (iii) the availability of reasonable and less trade-restrictive alternatives.[222]

The first step of the necessity test is assessing the relative importance of the interests and values underlying the Chinese VPN measure. The Chinese government has categorically argued that maintaining a stable internet, free from politically offensive and culturally harmful material is an important part of its domestic policy.[223] Similarly, the Chinese government has clearly emphasized the utmost importance of cybersecurity in domestic governance.[224] Therefore, a panel is likely to accord high priority and importance to these policy objectives. In fact,

---

222. Appellate Body Report, *Brazil – Measures Affecting Imports of Retreaded Tyres*, ¶ 146, 178, WTO Doc. WT/DS332/AB/R (adopted Dec. 17, 2007); US – Gambling AB Report, *supra* note 106, ¶ 307; Appellate Body Report, *Korea – Measure Affecting Imports of Fresh, Shilled and Frozen Beef*, ¶ 164, 166, WTO Doc. WT/DS161/AB/R (adopted Jan. 10, 2001).

223. *See generally* INFO. OFF. OF THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, THE INTERNET IN CHINA (June 8, 2010), http://china.org.cn/government/whitepaper/node_7093508.htm. *See also* INTERNET SOC. OF CHINA, PUBLIC PLEDGE OF SELF-REGULATION AND PROFESSIONAL ETHICS FOR CHINA INTERNET INDUSTRY (July 19, 2002), http://www.isc.org.cn/english/Specails/Self-regulation/listinfo-15321.html.

224. *See generally* Rogier Creemers, Paul Triolo, & Graham Webster, *Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference*, NEW AMERICA (Apr. 30, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

the AB has previously held that the "more vital or important the common interests or values pursued, the easier it would be to accept as 'necessary' measures designed to achieve those ends."[225] This would mean that in conducting the balancing test, a panel would likely consider the critical importance of online content regulation in China and ensure that it does not interpret the WTO rules in a manner that prevents the Chinese government from achieving this objective.

The second step is conducting the balancing test in GATS art. XIV. Importantly, this test requires the Panel to conduct an objective analysis of the measure.[226] The Panel would first determine whether imposing stringent requirements for registered VPN users and banning unauthorized VPN services contributes to any of the stated policy objectives found in step one. In conducting the analysis, the Panel can look at both qualitative and quantitative evidence, as well as the design and expected operation of the measure, especially since the measure is relatively new.

Given that VPN services are the primary tools for internet users in China to circumvent the firewall, the restriction on unauthorized VPN services would automatically reduce access to banned content thus, directly contributing to China's public policy goals GATS art. XIV(a). Further, as the Chinese VPN measure strictly requires service suppliers to track user activity through a centralized user archive, even users of authorized VPN services are likely incentivized to not violate domestic censorship laws and regulations.[227] Finally, as mentioned earlier, some experts argue that prohibiting the use of unauthorized VPN networks is central to shielding the networks from malicious actors and unwanted cyber intrusions.[228] Almost no information is publicly available regarding the effectiveness of the Chinese VPN measure in achieving online censorship and improving network security. Even so, the Chinese government, under GATS art. XIV, could still logically make these arguments to demonstrate that the Chinese VPN measure contributes to the government's policy objectives.

---

225. *EC—Asbestos AB Report*, *supra* note 156, ¶ 172 (internal quotations removed).

226. *See, e.g.*, US – Gambling AB Report, *supra* note 106, ¶ 304–308.

227. Chinese VPN Measure, *supra* note 13.

228. Rutkowski, *supra* note 215.

The second consideration in the balancing test is the level and extent that the Chinese VPN measure would restrict trade. The Chinese VPN measure is likely to have a strong detrimental impact on foreign companies by reducing their operational efficiency as well as inhibiting the security and privacy of their business transactions.[229] The US, in a submission to the WTO, stated:

> The potential impact of the Circular both on foreign service suppliers and their customers in China appears to be quite severe. Leased lines and VPNs are commonly used to ensure the security and confidentiality of information transferred into and out of a country in the course of supplying services. For example, to the extent that it relied on such services, how might a travel agent based in China access international flight information without connecting to a foreign data center? How could data processing or accounting services be supplied on a cross-border basis to Chinese clients/customers without some connection to a foreign data center? As another key example, many software platforms enable text messaging for technical support and customer service purposes – how would an online "chat" between a foreign accounting firm and its client in China, provided over a VPN or leased line be treated for the purpose of the Circular?[230]

Indirectly, this measure also favors domestic companies since the majority of foreign companies likely use cloud services in their regular business operations that remain blocked in China.[231] For example, press reports indicate that the demand

---

229. *Measures Adopted and Under Development by China Relating to its Cybersecurity Law*, *supra* note 170, ¶ 3, 5–6; *see also* Liza Lin & Yoko Kubota, *China's New Cyber Rules Add to Cost of Doing Business There*, WALL ST. J. (Mar. 30, 2018), https://www.wsj.com/articles/chinas-new-cyber-rules-add-to-cost-of-doing-business-there-1522397885; U.S. TRADE REPRESENTATIVE, 2020 REPORT TO CONGRESS ON CHINA'S WTO COMPLIANCE 59 (2021).

230. *Measures Adopted and Under Development by China Relating to its Cybersecurity Law*, *supra* note 170, ¶ 5.

231. For list of blocked websites, apps, and cloud services in China, *see* Kristina Perunicic, *The Complete List of Blocked Websites in China & How to Access Them*, VPN MENTOR (Jan. 18, 2022), https://www.vpnmentor.com/blog/the-complete-list-of-blocked-websites-in-china-how-to-access-them/. *See also* Alexander Chipman Koty, *China's Great Firewall: Business Implications*, CHINA BRIEFING (June 1, 2017), http://www.china-briefing.com/news/chinas-great-firewall-implications-businesses/.

for Chinese search engines, such as Baidu, has increased considerably after the measure came into effect.[232]

After the implementation of the measure, VPN services available in China are also arguably less secure because these service suppliers maintain a centralized user archive, which the government can use to track VPN users, access confidential business communications, and even conduct cyber-espionage. Whether the government does so in practice is uncertain, but a possibility remains that the measure could be implemented in this manner. If so, it would defeat the very purpose of VPN services of achieving access to a secure and private network. In a real dispute, however, consideration of these factors would depend on the evidence that the complainant(s) and third parties produce before the Panel.

In highly restrictive political environments such as China, VPNs are important in maintaining cross-border commercial activity without compromising the security and confidentiality of data flows. Further, the lack of sufficiently secure and trustworthy VPN services within China for intra-corporate communications can prevent foreign companies with strict corporate policies on privacy and security from operating in China altogether. Industry reports indicate various practical problems faced by foreign companies in China due to inconsistent blocking of VPN services and throttling of foreign websites.[233] Some software firms have also reported the various difficulties in selling software services in China because of the VPN measure.[234] Further, the cost of leasing MIIT-approved VPN services is significantly higher than other non-authorized services.[235] By limiting the choice of available legal VPN services in China, the VPN measure can create an enormous trade-restrictive impact across several sectors of the economy.

The last step in the necessity test is determining the availability of alternative measures that are less trade-restrictive but would equally advance the stated policy objectives, i.e., prohibiting the Chinese public from using unauthorized VPN services

---

232. *See* Ralph Jennings, *How to Surf China's Internet Freely Despite The Latest Ban*, FORBES (Apr. 23, 2018, 6:00 AM), https://www.forbes.com/sites/ralphjennings/2018/04/23/heres-how-to-surf-chinas-internet-freely-despite-the-latest-ban/#1d3e860e2934.

233. ITIF, *supra* note 30, at 8.

234. *Id.* at 12–14.

235. *Id.*

for illegal purposes. Here, the panel would only evaluate less trade-restrictive alternative measures that a complainant brings forward in a dispute. Further, such measures should be "reasonably available" to the defendant.[236] For instance, a complainant could propose that foreign businesses should be allowed to access any VPN service (licensed or unlicensed) for their corporate functions to reduce the potential adverse economic effects of the Chinese VPN measure. China, however, could argue that this measure is not reasonably available as the cost of monitoring such use would be disproportionate and perhaps infeasible. Thus, such a measure is only theoretical and not practical.[237] Further, if the objective is to control the activities of malicious actors in private, encrypted networks, such an alternative would not achieve the required level of protection. While the test of equivalent protection is not a proportionality test *stricto sensu*,[238] the Chinese VPN measure facilitates much stronger governmental supervision of authorized VPN services. Further, the efficacy of the above alternative is neither tested nor ascertainable.

Similarly, if China relaxed its requirement to maintain a user database for authorized VPNs to allay some of the concerns of foreign businesses regarding corporate espionage and corporate confidentiality, certain illegal uses may go unnoticed, thereby defeating the objective behind the Chinese VPN measure. China is likely to argue that stringent implementation of the Chinese VPN measure is necessary to achieve its desired level of protection.[239] Therefore, it remains possible for China to provisionally justify its VPN measure under GATS art. XIV.

3. Compliance with the General Exception Chapeau

To justify the Chinese VPN measure under GATS art. XIV, China would need to show that the measure meets the requirements of the chapeau of GATS art. XIV:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like

236. *EC—Asbestos AB Report*, *supra* note 156, ¶ 170–71.
237. *EC – Seal Product AB Report*, *supra* note 198, ¶ 5.261.
238. LESTER, MERCURIO & DAVIES, *supra* note 190, at 384.
239. *Cf.* China — Publications and Audiovisual Products AB Report, *supra* note 114, ¶ 318–19.

> conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures . . . .

The chapeau requires an assessment of how a measure is implemented rather than the content of the measure, which is instead examined under the sub-clauses of GATS art. XIV.[240] This assessment is necessary to examine whether a member is invoking the exception in good faith,[241] and not as a "disguised means of discrimination" against other Members.[242] Although the chapeau remains crucial as a defense, it is often unclear how it should be interpreted in practice.[243]

The first test under the chapeau is examining if 'like' conditions prevail in China, and in countries whose suppliers are prevented from offering VPN services in China, and if so, whether the measure results in arbitrary or unjustifiable discrimination. China can argue that its political and social culture is unique and other countries do not have "like" conditions regarding online censorship. For example, unlicensed VPN services supplied from abroad may not impose the same standards of censorship, security or restrictions on internet users as state-owned companies. In that case, the first condition of the chapeau is satisfied, as "like conditions" do not prevail in China and other Members. However, it is possible that VPN suppliers from certain Members agree to Chinese conditions for online censorship and oversight of internet users, in which case, the conditions in China and those Members will be "like."

If regulatory conditions are 'like', the panel would next investigate whether the Chinese VPN measure is applied in a manner that constitutes an arbitrary or unjustifiable discrimination.[244] For example, if China deliberately and unvaryingly rejects applications from foreign VPN suppliers proposing to form JVs with local partners, without any reasonable basis, then it would be a case of an arbitrary or unjustifiable discrimination.

---

240. *US—Gambling Panel Report*, *supra* note 130, at ¶ 6.607; *US—Gasoline AB Report*, *supra* note 130, at 22.

241. *US—Shrimp AB Report*, *supra* note 130, at ¶ 158.

242. LESTER, MERCURIO & DAVIES, *supra* note 190, at 374; *see, e.g.*, US – Gambling AB Report, *supra* note 106, ¶ 22.

243. Lorand Bartels, *The Chapeau of the General Exceptions in the WTO GATT and GATS Agreements: A Reconstruction*, 109 AM. J. INT'L L. 95, 96 (2015).

244. US – Gambling AB Report, *supra* note 106, ¶ 339.

Insufficient evidence is publicly available to make such an assertion. Given that all international VPN services currently available in China are offered by state-owned telecommunications companies, it is possible that a complainant can provide evidence of an arbitrary or unjustifiable discrimination, such as by collecting systematic evidence from service suppliers that have unsuccessfully attempted to obtain a license to supply VPN services in China. In the past, however, Telstra (an Australian company) was successful in 2015 in partnering with Pacnet Business Solutions China, a provider of IP-VPN services in China.[245] Further, as discussed earlier, the BT Group (a British company) was able to obtain a license for providing domestic VPN services in China in 2019.

In assessing whether there is arbitrary or unjustifiable discrimination, the Panel would ideally need evidence of discriminatory intent and not just discriminatory effect.[246] Depending on the evidence presented by the parties, the Panel could consider various factors: the security concerns of foreign VPN services and their ability to adhere to Chinese standards regarding online censorship; the reasons why certain foreign VPN service providers may have been unable to successfully receive MIIT approval to provide VPN services in China; and the rationale behind treating providers of international VPN services as BTS providers.

A complainant may also be able to adduce evidence that the Chinese VPN measure breaches the second condition of the GATS art. XIV chapeau, i.e., the measure constitutes a "disguised restriction on trade in services." This condition is met if the measure is implemented in such a manner that it protects domestic companies instead of pursuing any legitimate policy objective. An example of disguised restriction on trade would be that the Chinese government deliberately hampers the speed and efficiency of foreign VPN services to boost business of domestic companies. Some studies indicate that, in the past, the

245. Brian Karlovsky, *Telstra Expands Network into China with Pacnet Business Solutions*, ARN NET (May 11, 2015), https://www.arnnet.com.au/article/574641/telstra-expands-network-into-china-pacnet-business-solutions/.

246. LESTER, MERCURIO & DAVIES, *supra* note 190, at 432.

Chinese government has throttled foreign VPNs.[247] This action would constitute a disguised restriction on trade.

Further, if the Chinese VPN measure restricted several unlicensed foreign VPN services but did not impose similarly stringent requirements on domestic VPN services, then this would also constitute a disguised restriction on trade.[248] A panel may also take into account that certain domestic Chinese companies, such as Baidu, Weibo and WeChat, were able to prosper immensely due to the lack of foreign competition, which can arguably also be attributed to the lack of reliable VPN services in China.[249] Thus, if a party is able to provide specific evidence outlining the discriminatory aspects in the implementation of the Chinese VPN measure, it can satisfy the threshold under GATS art. XIV chapeau.[250]

Therefore, even though governments enjoy regulatory autonomy under GATS art. XIV to implement measures to achieve domestic policy objectives, they cannot escape their GATS obligations if they disguise blatantly protectionist measures as being essential to achieve domestic public policy objectives. GATS art. XIV thus plays an important role in drawing a fine line between measures that protect domestic policy objectives and those that are blatantly protectionist and defeat the very purpose of WTO laws.

III. INTERNATIONAL TRADE LAW AND ONLINE CONTENT REGULATION: TOWARDS AN OPEN INTERNET

The interface of international trade law and online content regulation entails both economic and non-economic considerations. Online content regulations implicate various social issues including promoting freedom of expression and access to information, protection of minorities, and regulation of harmful online content such as fake news, disinformation and hate speech. Concurrently, from an economic perspective, online content regulation can harm digital trade flows and potentially

247. Margaret Earling Roberts, Fear, Friction, and Flooding: Methods of Online Information Control 3 (2014) (Doctoral dissertation, Harvard University), https://dash.harvard.edu/handle/1/12274299.

248. *See generally* Cho-Wen Chu, *Censorship or Protectionism? Reassessing China's Regulation of Internet Industry*, 7 INT'L J. SOC. SCI. & HUMAN. 28 (2017).

249. Zhen, *supra* note 34, at 742; Chu, *supra,* note 250, at 28–31.

250. *Id*.

breach obligations contained in international trade agreements, as demonstrated above in Section III.

Given this interface, at first sight, it appears normatively appealing to argue that international trade law can be an instrument to promote a free internet, enable free flow of information, and promote human rights. As discussed above, however, doing so may open a can of worms for trade tribunals and force them to deal with issues that are both sensitive and clearly outside their expertise. Further, as Broude and Hestermeyer argue, international trade law is indifferent to human rights and only deals with economic effects of online censorship, something that is neither sufficient nor fruitful in dealing with the broader policy concerns at the heart of online content regulation.[251] It can also potentially be dangerous and counterproductive to push for a human rights agenda through trade tribunals.[252] In particular, using exceptions in international trade agreements to advance the agenda of a free and open internet can become a double-edged sword. On one hand, if the WTO adopts a strict standard of review in evaluating the normative content of a measure (e.g., does a majority of the country agree with the ruling party's idea of online censorship?), then it needs to judge issues that fall outside its competence. On the other hand, if it is highly deferential to any policy objectives that the government states as being the rationale behind the measure, then it may inadvertently open the gates to protectionist behavior.[253]

The article argues that international trade law must preserve Members' sovereignty to pursue their cultural, political, and social goals, and thus should only interfere with online content regulatory measures to the extent that there is evidence of disguised protectionism. In particular, it argues that a trade tribunal is not in a favorable position to assess whether a measure is normatively sound (for example, is it in the interests of public order or public morality to prevent citizens from accessing online information, or is it merely the wishes of the ruling political

---

251. Tomer Broude & Holger Hestermeyer, *The First Condition of Progress? Freedom of Speech and the Limits of International Trade Law*, 54 VA. J. INT.'L L. 295, 295 (2015).

252. Philip Alston, *Resisting the Merger and Acquisition of Human Rights by Trade Law: A Reply to Petersmann*, 13 EJIL 815, 833-836 (2002).

253. Nicolas F. Diebold, *The Morals and Order Exceptions in WTO Law: Balancing the Toothless Tiger and the Undermining Mole*, 11 J. INT'L ECON. L. 43, 44 (2007).

party?). Similarly, trade tribunals may need to acknowledge that certain regulations are genuinely aimed at enhancing security or integrity of networks and any resulting trade-restrictive impact is purely incidental. Further, countries have variable regulatory capacities and may lack the resources to adopt the least trade-restrictive regulatory tools, such as selective filtering of websites instead of en masse blocking of specific services or websites.[254]

This does not mean that trade tribunals are bereft of any tools to curb protectionist measures that are carefully disguised as being necessary to protect domestic policy objectives. The principles embedded in international trade agreements such as nondiscrimination, market access, and transparency can be relevant in assessing the reasonableness and effectiveness of online content regulations and ensuring that they are devoid of any blatant protectionist intent. For instance, under the WTO framework, countries must impose only proportional and objective technical standards on services;[255] must be able demonstrate the causal connection between their regulatory measure and its underlying policy objective; and should employ the least trade-restrictive means that is reasonably available to achieve their domestic policy objectives.[256]

An incidental impact of scrutinizing measures related to online content regulation under international trade law could be promoting certain human rights and human freedoms aligned with (Western) democratic values.[257] But the WTO cannot act as a forum for setting transnational norms or standards on online censorship or content regulation, nor can it force all its Members to adopt a free and open internet.[258] Therefore, despite growing concerns regarding the intrusive nature of trade agreements[259] and the seemingly close relationship of digital trade and online censorship, existing trade rules cannot become tools to bring

254. *See generally* Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 CHI. J. INT'L L. 12 (2006).

255. GATS, *supra* note 12, arts. VI(5), VI(4). *See also* Erixon, Hindley & Lee-Makiyama, *supra* note 42, at 14.

256. See discussion in Section IVE.

257. *See generally* Chander, *supra* note 16.

258. Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7(1) CHI. J. INT'L L. 263, 276-287 (2006).

259. Jorg Mayer, *Policy Space: What, For What and Where?* 1 (UNCTAD, Discussion Paper No. 191, 2008), https://unctad.org/system/files/official-document/osgdp20086_en.pdf.

down digital walls that sovereign countries build to regulate their online environment for legitimate reasons.

Instead, limiting digital protectionism requires transnational consensus and shared norms.[260] In the ongoing plurilateral negotiations on electronic commerce under the Joint Statement Initiative of the WTO, several countries have proposed disciplines to prohibit data localization and promote the free flow of data for digital trade.[261] These disciplines also contain exceptions (worded somewhat similar to the WTO exceptions) that would preserve the right of countries to regulate their domestic internet for "legitimate domestic public policy objectives,"[262] arguably covering domestic measures related to online content regulation. Similar provisions can also be found in recent Electronic Commerce or Digital Trade Chapters in FTAs.[263]

Norms that develop outside of trade institutions can bring greater certainty and regulatory coherence to global online content regulations. For instance, like-minded countries could agree to encourage the use of least intrusive methods to inhibit circulation of online content, such as through bilateral arrangements and understandings, or develop common standards in certain areas, such as disinformation regulation.[264] In 2021, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression presented a report to the Human Rights Council regarding the human rights implications of disinformation and possible responses to these concerns, both at the multilateral and multistakeholder level.[265] The United Nations General Assembly has also taken note of the human rights

260. Susan Ariel Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, 18 WORLD TRADE REV. 541, 543 (2019).

261. *Joint Initiative on E-commerce*, WTO, https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm (last visited Nov. 25, 2022).

262. Panel Negotiations, *WTO Electronic Commerce Negotiations*,at 28] WTO Doc. INF/ECOM/62/Rev.1 (Dec. 14, 2020), https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf.

263. *See, e.g.*, Comprehensive and Progressive Agreement for Trans-Pacific Partnership arts. 14.11.3, 14.13.3, Mar. 8, 2018, TPP-11.

264. European Commission Press Release UP/21/2990, EU-US Launch Trade and Technology Council to Lead Values-Based Global Digital Transformation (June 15, 2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990.

265. U.N. Human Rights Council, *Disinformation and freedom of opinion and expression*, U.N. Doc. A/HRC/47/25 (Apr. 13, 2021), https://undocs.org/A/HRC/47/25.

repercussions of the ongoing "infodemic" and the ways in which the international community can cooperate to reduce the spread of disinformation.[266] Some experts also argue that high-level agreements, such as the *Digital Economy Partnership Agreement,* could also help countries fight global problems like disinformation.[267]

Nonetheless, it is important to remain cautiously optimistic regarding such endeavors, especially in the short run. Several international and multistakeholder initiatives on the regulation of cyberspace have had limited impact,[268] including the Digital Geneva Convention,[269] Paris Call for Trust and Cybersecurity in Cyberspace,[270] and the Global Commission on the Stability of Cyberspace.[271] Further, the normative and ideological differences among countries on the human rights implications of online censorship are not easily resolvable, especially where significant socio-cultural differences exist. Nonetheless, it remains possible that deliberations in non-trade fora on issues such as disinformation may bring more regulatory coherence in online content regulation across countries, and in turn facilitate the breaking down of digital trade barriers.

---

266. U.N. GAOR, 76th Sess., 11th & 12th plen. Mtg., U.N. Doc. GA/SHC/4338 (Nov. 15, 2021), https://www.un.org/press/en/2021/gashc4338.doc.htm.

267. *See generally* Susan Aaronson, *Can Trade Agreements Solve the Wicked Problem of Disinformation*, (Inst. for Int'l Econ. Pol'y, Working Paper IIEP-WP-2021-12, 2021), https://iiep.gwu.edu/2021/04/26/can-trade-agreements-solve-the-wicked-problem-of-disinformation/.

268. Duncan Hollis, *A Brief Primer on International Law and Cyberspace*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (June 14, 2021), https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763; Christian Ruhl et al., Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Feb. 26, 2020), https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

269. *See generally* Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT ON THE ISSUES (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

270. PARIS CALL: FOR TRUST AND SECURITY IN CYBERSPACE (2018), https://pariscall.international/en/call (last visited Nov. 25, 2022).

271. *The Commission*, GLOB. COMM'N ON THE STABILITY OF CYBERSPACE, https://cyberstability.org/about/ (last visited Nov. 25, 2022).

CONCLUSION

This Article explored the growing interaction of digital trade and online content regulation through the lens of a measure restricting unlicensed VPN services in China. It argued that while certain aspects of the Chinese VPN measure may be inconsistent with Chinese commitments under the GATS on VPN services, China is quite likely to succeed (at least provisionally) in defending its measure as being necessary for protecting various policy objectives contained in GATS art. XIV. In the absence of international norms on online censorship and the lack of unanimity regarding the technological effectiveness of various online content regulatory methods, any trade tribunal will likely face several limitations in scrutinizing the policy rationale behind the measure and assessing alternatives that may be less trade restrictive.

The case study also indicated that WTO laws provide certain tools to the Panels to investigate the causal connection between a particular measure and that country's stated online content regulatory goals. Further, a complainant may be able to provide evidence regarding a particular online content regulatory measure being implemented in an inconsistent and arbitrary manner, thereby violating WTO laws. Such a measured approach in applying international trade law to domestic digital regulation is pragmatic and judicious. It also preserves the spirit of WTO laws that protects Members' right to regulate. Further, it does not conflate the economic liberalization objective of international trade law with the multifaceted socio-economic aspects of online content regulation.

Rising digital walls are undesirable, harmful, and counterproductive. Thus, a transnational consensus on online content regulation is both important and urgent. Such consensus is best developed through mature bilateral understandings (including outside conventional international treaties), robust self-regulatory codes in the private sector, and meaningful dialogues in the transnational and multi-stakeholder fora, rather than at the WTO or other trade institutions. Greater consensus among countries regarding online regulation will instill trust, openness, and regulatory coherence in global digital trade, which in turn helps break down digital trade barriers. However, certain deep-seated, irresolvable ideological differences regarding online content regulation will remain, and it is perhaps judicious for trade policymakers and tribunals to leave them untouched.

GAT
S/SC/
135

Sector or sub-sector	Limitations on market access	Limitation on national treatment	Additional commitments
C. Telecommunication Services[3] Value-added Services Including the following:	(1) See mode 3 (2) None (3) Foreign service suppliers will be permitted to establish joint venture value-added telecommunication enterprises, without quantitative restrictions, and provide services in the cities of Shanghai, Guangzhou and Beijing. Foreign investment in joint venture shall be no more than 30 per cent. Within one year after China's accession, the areas will be expanded to include Chengdu, Chongqing, Dalian, Fuzhou, Hangzhou, Nanjing, Ningbo, Qingdao, Shenyang, Shenzhen, Xiamen, Xi'an, Taiyuan and Wuhan and foreign investment shall be no more than 49 per cent. Within two years after China's accession, there will be no geographic restriction and foreign investment shall be no more than 50 per cent. (4) Unbound except as indicated in horizontal commitments.	(1) None (2) None (3) None (4) Unbound except as indicated in horizontal commitments.	China undertakes the obligations contained in the Reference Paper in Annex I attached hereto.
(h) Electronic mail			
(i) Voice mail			
(j) On-line information and database retrieval			
(k) Electronic data interchange			
(l) Enhanced/Value-added facsimile services (including store and forward, store and retrieve)			
(m) Code and protocol conversion			
(n) On-line information and/or data processing (including transaction processing)			

(5) Annex: Extract of Chinese Schedule Containing China's Commitments on Telecommunications and Computer Services

- Basic Telecommunication Services - Paging Services	(1) See mode 3 (2) None (3) Foreign service suppliers will be permitted to establish joint venture enterprises, without quantitative restrictions, and provide services in and between the cities of Shanghai, Guangzhou and Beijing. Foreign investment in joint venture shall be no more than 30 per cent. Within one year after China's accession, the areas will be expanded to include services in and between Chengdu, Chongqing, Dalian, Fuzhou, Hangzhou, Nanjing, Ningbo, Qingdao, Shenyang, Shenzhen, Xiamen, Xi'an, Taiyuan and Wuhan and foreign investment shall be no more than 49 per cent. Within two years after China's accession, there will be no geographic restriction and foreign investment shall be no more than 50 per cent. (4) Unbound except as indicated in horizontal commitments.	None None None Unbound except as indicated in horizontal commitments.	China undertakes the obligations contained in the Reference Paper in Annex 1 attached hereto.

- Domestic Services (a) Voice services (b) Packet-switched data transmission services (c) Circuit-switched data transmission services (f) Facsimile services (g) Domestic private leased circuit services - International Services (a) Voice services (b) Packet-switched data transmission services (c) Circuit-switched data transmission services (f) Facsimile services (g) International closed user group voice and data services (use of private leased circuit service is permitted)	(1) See mode 3 (2) None (3) Within three years after China's accession, foreign service suppliers will be permitted to establish joint venture enterprises, without quantitative restrictions, and provide services in and between the cities of Shanghai, Guangzhou and Beijing. Foreign investment in the joint venture shall be no more than 25 per cent. Within five years after accession, the areas will be expanded to include services in and between Chengdu, Chongqing, Dalian, Fuzhou, Hangzhou, Nanjing, Ningbo, Qingdao, Shenyang, Shenzhen, Xiamen, Xi'an, Taiyuan and Wuhan. And foreign investment shall be no more than 35 per cent. Within six years after accession, there will be no geographic restriction and foreign investment shall be no more than 49 per cent. (4) Unbound except as indicated in horizontal commitments.	(1) None (2) None (3) None (4) Unbound except as indicated in horizontal commitments.	

GAT
S/SC/
135

B. **Computer and Related Services**			
(a). Consultancy services related to the installation of computer hardware (CPC 841)	(1) None (2) None (3) None (4) Unbound except as indicated in horizontal commitments.	(1) None (2) None (3) None (4) Qualifications are as follows: certified engineers, or personnel with Bachelor's degree (or above) and three years of experience in these fields.	