THE INAUGURAL JOHN D. GREENWALD WRITING COMPETITION: WINNING NOTE

READING THE TRADE TEA LEAVES: A COMPARATIVE ANALYSIS OF POTENTIAL UNITED STATES WTO-GATS CLAIMS AGAINST PRIVACY, LOCALIZATION, AND CYBERSECURITY LAWS

JOSHUA D. BLUME*

ABSTRACT

For the first twenty-plus years of the WTO, the vast majority of cases brought before the Appellate Body have been grounded on General Agreement on Tariffs and Trade ("GATT") claims. Over the twenty years of the WTO's life, however, digital trade and cross-border data flows have grown from nearly non-existent to larger in volume and gross product value than trade in goods. As digital trade has accelerated to more than $400 billion each year, many countries have attempted to erect barriers that protect domestic industry while attempting to claim exceptions to the General Agreement on Trade in Services ("GATS"). These justifications range from protections for citizens' privacy, ensuring cybersecurity, and strengthening national security. As a major exporter of digital services trade, the United States would greatly benefit from bringing a case against at least one of these countries to remove or revise the restrictive laws and regulations. Three WTO members, namely the European Union, China, and Russia, not only have such laws and regulations, they have also created those laws based on questionable logic and assumptions. This Note will start by analyzing the individual WTO and GATS commitments made by Russia, China, and the EU. It will then scrutinize applicable WTO case law under the GATS, as well as the Russian localization, EU privacy, and Chinese cybersecurity laws. These laws are then compared with the language of the WTO and GATS, as well as other trade agreements to which the countries are party. Finally, the Note will

* Joshua D. Blume graduated from the Juris Doctor program at Georgetown University Law Center in May 2018, with a Certificate in WTO Studies. During his time at Georgetown Law, Joshua served as the Trade Editor for the Georgetown Journal of International Law. Joshua holds a B.A. with double majors in Economics and International Studies with minors in Classical Studies and Political Science from Utah State University. He would like to thank his wife, Kolbie for all her love and support, Senator Hatch for giving him a chance, the editors and staff of the Georgetown Journal of International Law for their time and assistance, and all of the other friends, family, and coworkers who helped him with both the genesis of this note and life more generally.

conclude by summarizing the likelihood of success the United States would have in complaints against each of the three WTO members.

I. Introduction

According to a recent report by the McKinsey Global Institute, "cross-border data flows now generate more economic value than traditional flows of traded goods."[1] While different in many ways, digital and physical goods both face barriers to trade. Digital barriers are often erected by states to provide domestic protections, increase national security, and assert human rights and consumer protections. One estimate finds that these barriers currently threaten around $400 billion (USD) in trade each year.[2] Two of the most prominent barriers to data-flows trade are data localization,[3] and privacy and data security restrictions.[4] These barriers increase costs to consumers and often restrict access to content available elsewhere on the globe. One way that the United States could encourage other states to increase the free-flow of data

1. James Manyika et al., Digital Globalization: The New Era of Global Flows 2 (2016).

2. David J. Lynch, *The U.S. dominates the world of big data. But Trump's NAFTA Demands Could Put that at Risk*, Washington Post (Nov. 28, 2017), https://www.washingtonpost.com/business/economy/trumps-trade-deficit-obsession-could-hurt-leading-american-industries/2017/11/27/b2b8122c-cbb5-11e7-8321-481fd63f174d_story.html?utm_term=.3bee4dab0ca0.

3. *Fact Sheet: Key Barriers to Digital Trade*, U.S. Trade Representative (Mar. 2016), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade.

4. *See* Manyika et al., *supra* note 1, at 17-18; Press Release, BSA, Modernizing Trade for NAFTA and Beyond (May 22, 2017), http://www.bsa.org/news-and-events/news/2017/may/en05222017-modernizing-trade-for-nafta-and-beyond?sc_lang=en-US&gclid=Cj0KCQjw1dDPBRC_ARIsAJZrQfq9JUYAvrRZFaLB8HXeeaAAjewgKcSng4pnHkjq8QHOOwVFXP9fuBAaAglZEALw_wcB; *see also European Union – Data Privacy and Protection*, Export.gov (Jul. 19, 2017), https://www.export.gov/article?id=European-Union-Data-Privatization-and-Protection (for specific references to the EU GDPR).

would be by bringing a complaint before the World Trade Organization against countries with restrictive laws and regulations. In its complaint, the United States could specifically argue that the General Agreement on Trade in Services ("GATS") had been violated by those countries with data restricting laws and regulations. Bringing down these types of data localization and privacy laws through a GATS challenge would be an unprecedented move by any WTO member, and would require sophisticated arguments aimed with precision to avoid collateral damage to defenses often asserted and protected by the United States. This Note looks at the likelihood of success that such a challenge would have on three major laws:[5] the European Union General Data Protection Regulation ("GDPR"),[6] the Russian data localization law,[7] and the Chinese Cyber-Security law.[8] This Note concludes by finding that each of the laws in China, Russia, and the EU analyzed in the following sections would be found in violation of Articles VI, XVI, and XVII by the WTO Appellate Body. Furthermore, any attempt to use an Article XIV or Article XIV *bis* defense would most likely fail as well for each of the three WTO members, though the EU would have the strongest defense of the three so long as the individual member states refrain from localizing data.

II. Defining the Parameters

Prior to identifying the applicable GATS provisions, it is first necessary to demonstrate that the types of applicable services are, indeed,

5. These three laws were chosen for their polarizing impact; for a more complete list of restrictive laws globally see *International Data Flows: Promoting Digital Trade in the 21st Century: Before the H. Subcommittee on Courts, Intellectual Property, and the Internet*, 115th Cong. 5 (2015) (statement of Ed Black, President & CEO, the Computer & Communications Industry Association).

6. Parliament and Council Regulation 2016/679 of May 4, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

7. *See* Polly Mosendz, *Newly Signed Law Could Give Putin Total Control of Russia's Internet*, Atlantic (May 6, 2014), https://www.theatlantic.com/international/archive/2014/05/newly-signed-law-could-give-putin-total-control-of-russias-internet/361819/; *see also* Paul Sonne & Olga Razumovskaya, *Russia Steps Up New Law to Control Foreign Internet Companies; Move Seen as Part of Drive to Curtail Freedom of Information*, Wall Street J. (Sept. 24, 2014, 12:08 PM), https://www.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920.

8. *See* Leigh Ann Ragland et al., Center for Intelligence Research and Analysis, Red Cloud Rising: Cloud Computing in China (Sep. 5, 2013, revised Mar. 22, 2014); *see also* Information Technology Industry council (ITI), Data Localization Snapshot (current as of Jan. 19, 2017) (citing that the law requires "local processing and storage of 'important data' related to Chinese citizens and critical information infrastructure").

covered by the GATS. When the WTO was created, the General Agreement on Tariffs and Trade ("GATT") was revised and coupled with other agreements to provide a broader scope for international trade that would include services instead of just goods.[9] Because the GATT only governed the trade of goods, WTO members had felt it was important to sign a new agreement to cover services, called the GATS.[10] While some authors have taken the position that data may, in fact, be covered by the GATT,[11] such a position might constrain the number of companies that can claim damages under the GATS.[12] Instead, this Note focuses on data flows broadly, with an eye specifically to means of transfer and the types of laws and regulations that actively prohibit transfers on a broad scale. Furthermore, this Note does not treat the data flows of "big data" any differently than intra-company human resource data transfers.[13] This is because thousands of companies within the United States rely on their ability to easily transfer information back to the United States, both for their customer base, as well as for their current employees.[14]

Furthermore, as noted by Mara Burri, this Note recognizes the difference between the broad computer and related services commitments under the GATS, and infers that because telecommunications providers must ultimately deliver the individual data packets, Russia, China, and the EU member states will be more likely to push the debate toward the telecommunications sector commitments they have made, which include far more exemptions and caveats comparatively.[15] Not wanting to shy away from the most likely area of debate, this Note will analyze the broad commitments made in the telecom space alone, and

9. General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194 [hereinafter GATT]; *The GATT Years: from Havana to Marrakesh*, WTO, https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact4e.htm (last visited Dec. 15, 2017).

10. *See* Sandra Anderson, *General Agreement on Trade in Services: A Resource for Librarians*, U. OF ALTA., http://capping.slis.ualberta.ca/global/sandra/history.html (last visited Dec. 15, 2017).

11. *See* MARA BURRI, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C. DAVIS L. REV. 65 (2017).

12. This is because certain types of data may or may not be considered a good, and some of the barriers might not actually apply to the physical data itself. *See, e.g.*, JOSHUA MELTZER, *The Internet, Cross-Border Data Flows and International Trade*, 22 ISSUES IN TECH. INNOVATION 1, 14-16 (2013).

13. BURRI, *supra* note 11, at 67-68.

14. *See* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/list (last visited Dec. 18, 2017) (listing more than 2750 companies that currently rely on the Privacy Shield framework alone to transfer data back and forth between the United States and the EU).

15. *See generally* BURRI, *supra* note 11, at 84-85.

purely within the realm of the GATS.[16] Finally, it is key to understand that thousands of companies from dozens of sectors rely on the ability to simply transfer information between countries to fulfill their business.[17] This approach ensures that this Note gives full treatment to the more difficult arguments that are likely to be raised, while also encompassing the cross-border data flows that occur for thousands of different U.S. businesses.

III. GATS Provisions at Play

Because digital transfers are frequently considered trade in services,[18] this Note will analyze the legal basis of bringing a suit before the WTO under the applicable provisions of the GATS. As noted previously, some have argued that data may be included under the GATT, but typically, those authors make such arguments because the commitments under the GATT are considered stronger—not because the transfer of digital packets from one country to another would not be interpreted as a service.[19] As such, this Note considers only the GATS commitments of Russia, China, and the EU, as those commitments are more encompassing.[20]

A. *GATS Article I:2: Definition of Trade in Services*

GATS Article I:2 outlines the definition of cross-border "trade in services," in part, as providing a "cross border supply" of a service from a provider located in "the territory of one Member into the territory of

16. This is, again, the more difficult path to follow, as the Appellate Body found that the telecommunications agreement required broad and durable commitments from all applicable member states in the *Mexico – Telecoms* case; *see Summary of the Dispute at WTO, DS 204, Mexico – Measures Affecting Telecommunications Services*, WTO, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds204_e.htm (last visited Dec. 18, 2017).

17. *See generally* Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, Info. Tech. & Innovation Found. (May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.39529124.604133252.1523416793-1591259467.1523416793 (providing a broad overview of the broad impact many data flows barriers have, and how those barriers affect virtually any international business actors).

18. *See, e.g.*, Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, OECD Digital Econ. Papers No. 187, 15 (2011).

19. *See generally* Burri, *supra* note 11, at 84-85.

20. *Id.*; *see also, The General Agreement of Trade in Services (GATS): objectives, coverage, and disciplines*, WTO, https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm (last visited Dec. 18, 2017); *Services: rules for growth and investment*, WTO, https://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm6_e.htm (last visited Dec. 18, 2017); Juan A. Marchetti & Petros C. Mavroidis, *The Genesis of the GATS (General Agreement on Trade in Services)*, 22 European J. of Int'l L 689 (2011).

any other Member."[21] Data transfers and digital access are widely believed to fall under this provision with all subsequent rules applicable to these "services."[22] There are four modes of providing services under the GATS, which, when paired with the fundamental principles of market access[23] and national treatment,[24] create the tapestry of fundamental principles used by most nations to regulate international trade in services. The types of "service[s]" utilized for data transfer are further clarified in the Scheduling Guidelines, which provide that protections for cross-border supply of services apply to service providers "not present within the territory of the Member" and "service delivered within the territory of the Member from the territory of another Member."[25] This type of service transfer is also commonly known as "Mode 1" of the four modes of services transfers.[26] Through a Mode 1 analysis, data localization, privacy, and cyber-security requirements are most likely to be found in violation of the market access and national treatment provisions, as well as the "domestic regulation" restrictions in Article VI.[27]

B. *GATS Article VI: Proper Regulation*

In addition to the fundamental principles of national treatment and market access, the GATS also requires member states to recognize "the right of Members to regulate, and to introduce new regulations, on the supply of services within their territories in order to meet national policy objectives. . . ."[28] This provision in the preamble presupposes a tension between self-regulation and free trade.[29] Paragraph 2 of Article VI is also one of only four generally applicable provisions that do not require further commitment by members.[30] Instead, Paragraph 2

21. GATS: General Agreement on Trade in Services, art. I:2, Apr. 15, 1994, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994) [hereinafter GATS].

22. Daniel Crosby, *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, INTERNATIONAL CENTRE FOR TRADE AND SUSTAINABLE DEVELOPMENT 6 (Mar. 2016).

23. GATS art. XVI.

24. GATS art. XVII.

25. Scheduling Guidelines, S/L/92, 28 March 2001, para. 26 [emphasis in original].

26. Rolf H. Weber, *Regulatory Autonomy and Privacy Standards Under the GATS*, 7 ASIAN J. OF WTO & INT'L HEALTH L. AND POL'Y 25, 27 (2012).

27. *See generally* Weber *supra* note 26.

28. GATS preamb. § 4.

29. *See* Shin-yi Peng, *Digitalization of Services, the GATS and the Protection of Personal Data*, KOMMUNIKATION: FESTSCHRIFT FÜR ROLF H. WEBER ZUM 60 GEBURTSTAG 753, 763-64. (2011).

30. GATS GENERAL AGREEMENT ON TRADE IN SERVICES: A HANDBOOK FOR INTERNATIONAL BAR ASSOCIATION MEMBER BARS, INT'L B. ASS'N 9 (May 2002) *citing* Laurel S. Terry, *GATS' Applicability to Transnational Lawyers and its Potential Impact on Domestic Regulation of U.S. Lawyers*, 34 VAND. J. OF TRANSNAT'L L. 989 (2001) [hereinafter GATS Handbook].

requires that each member state institute proper tribunals or arbitral services, as constitutionally permissible, for affected service providers.[31] Paragraphs, 1, 3, 5, and 6, however, require specific commitments by each member in their corresponding schedules.[32] Those paragraphs require committing members to ensure "all measures of general application affecting trade in services are administered in a[n] . . . impartial manner" and that "each Member shall provide for adequate procedures to verify the competence of professionals of any other Member" where specific commitments regarding those professional services are taken.[33] These broad commitments have been considered somewhat restricted, however, by Paragraph 5, which acts as a type of "standstill" provision, ensuring that a Member's commitments be taken in the context in which the commitments were made.[34] Furthermore, per the Appellate Body's ruling in *U.S.–Gambling*, the analysis for domestic regulations commitments is treated in an entirely different provision from the market access commitments in Article XVI.[35] However, the Working Party on Professional Services has explained that there is significant interplay between GATS Articles XVI, XVII and VI.[36]

C. *GATS Article XVI: Market Access*

At its core, Article XVI is the GATS "market access" provision.[37] In essence, if a country lists a particular sector on its Schedule of Specific Commitments, that country must provide access to foreign supplies of that particular sector to its market.[38] This also requires that WTO members provide foreign suppliers treatment "no less favorable" than

---

31. GATS art. VI § 2.

32. *GATS General Agreement on Trade in Services: A Handbook for International Bar Association Member Bars*, INT'L B. ASS'N 19 (May 2002) *citing* Laurel S. Terry, *GATS' Applicability to Transnational Lawyers and its Potential Impact on Domestic Regulation of U.S. Lawyers*, 34 VAND. J. OF TRANSNAT'L L. 989 (2001).

33. GATS art. VI, §§ 1, 6.

34. GATS Handbook, *supra* note 30, at 20-21.

35. Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶¶ 25, 225, 252, WTO Doc. WT/DS285/26 (adopted Apr. 25, 2013) [hereinafter *US–Gambling*].

36. *See generally* WORKING PARTY ON PROFESSIONAL SERVICES, REPORT TO THE COUNCIL FOR TRADE IN SERVICES ON THE DEVELOPMENT OF DISCIPLINES ON DOMESTIC REGULATION IN THE ACCOUNTANCY SECTOR, WTO Doc. S/WPPS/4 (Dec. 10, 1998) (focusing, in large part, on licensing guidelines, requirements, and qualification exams for accountants).

37. GATS Handbook, *supra* note 30, at 18; *see also,* Panos Delimatsis & Martin Molinuevo, *Article XVI GATS: Market Access*, MAX PLANCK COMMENTARIES ON WORLD TRADE LAW, WTO–TRADE IN SERVICES 385-86 (Rüdiger Wolfrum et. al., eds., 2008).

38. GATS Handbook, *supra* note 30, at 18.

provided to domestic suppliers.[39] This Article has been seen as providing a restrictive approach, in other words, focusing "on what a WTO Member State may not do."[40] Importantly to data transfer, Footnote 8, contained in the original document, explains that when a market-access commitment has been made in a member's Schedule, the member has committed to the open flow of related services, such as capital transfers with respect to a broad commitment as movement of capital.[41] This was later confirmed, and is now referenced by the WTO as an instructive analysis much because it was not appealed, in *U.S.-Gambling*, when a WTO Panel asserted that a commitment "given for the supply of a service through mode 1 . . . applies to any mode of delivery in mode 1."[42] In sum, the market access provisions in Article XVI signifies that a foreign supplier must have access to the domestic market of a WTO member-state, so long as the member has made commitments to the related industry. However, because of the size and scope of digital transfers, this Note assumes that any commitments to a sector that can be supplied or enhanced by digital transfers would be included as well.

D. *GATS Article XVII: National Treatment*

The foundational principles of free flows of international trade have long included the doctrine of national treatment.[43] Article XVII is the national treatment rule, which requires countries to provide equal market access to foreign and domestic service providers so long as the member lists the service in its Schedule of Specific Commitments.[44] As the International Bar Association GATS Handbook explains, a member would violate its GATS commitments if it included, for example, lawyers in its schedule, but then utilized some method to alter market conditions and make it more difficult for foreign lawyers to practice.[45] Importantly for digital trade, however, is Footnote 10, which, as

39. *Id.*

40. *Id.*; *see also Misunderstandings and scare stories: Market access and national treatment commitments*, WTO, https://www.wto.org/english/tratop_e/serv_e/gats_factfiction6_e.htm (last visited Dec. 18, 2017) (refuting claims made by the World Development Movement in 2000 and further explaining the thrust of Article XVII).

41. GATS art. XVI n.8.

42. WTO ANALYTICAL INDEX: GATS – ARTICLE XVI (JURISPRUDENCE), WTO 4 (also note that as one of very few cases instructive on cross-border data supplies, the *U.S.–Gambling* case will be analyzed further below).

43. *Principles of the trading system*, WTO, https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm (last visited Dec. 18, 2017).

44. GATS Handbook, *supra* note 30, at 18.

45. *Id.*

included in the original text, specifies that members cannot use provisions to compensate for "any inherent competitive disadvantages which result from the foreign character of the relevant services or service suppliers."[46] In the case of the foreign lawyer, for example, native language fluency might not be allowed as a requirement of domestic law or regulation, but the government also need not assist in compensating for the foreign lawyer's linguistic deficiency. It should also be noted that while there is an important test for the "likeness" of a service,[47] the large scope and scale of the digital economy inevitably will create some overlap between otherwise dissimilar services. Therefore, because of the scope, scale, and variety of digital services, this Note accepts that there are likely to be many specific sectors and services that could be used to bring a complaint and no specific analysis is given to any one service over another. Furthermore, while each WTO Member is allowed to make exemptions to the most-favored-nation provisions in GATS Article II, this Note will not analyze these specific exemptions as it is an analysis tangential to the GATS articles more applicable to data transfers.[48]

IV. GATS Member-Specific Commitments in Context

As noted in foregoing sections on GATS Articles VI, XVI, and XVII, a WTO member state can only be held accountable for covered services.[49] The following sections analyze the relevant and broad commitments listed in the applicable schedules for the EU, Russia, and China.

A. *European Union*

In its original commitments, the EU cited no limitations on market access or national treatment for "telecommunications services," including data base retrieval.[50] This treatment in the initial list of commitments was not substantially altered when it was first revised in 1997 to specifically target the telecommunications services sections of the

46. GATS art. XVII, n.10.

47. *See* Appellate Body Report, *European Communities–Bananas III*, ¶ 7.322, WTO Doc. WT/DS27/AB/R (adopted Sept. 9, 1997).

48. *See, e.g.*, *List of Article II (MFN) Exemptions of the European Communities and their Member States*, WTO Doc. GATS/EL/31 (Apr. 15, 1994).

49. *See Guide to reading the GATS schedules of specific commitments and the list of article II (MFN) exemptions*, WTO, https://www.wto.org/english/tratop_e/serv_e/guide1_e.htm (last visited Dec. 18, 2017).

50. *European Communities and Their Member States - Schedule of Specific Commitments*, 50, WTO Doc. GATS/SC/31 (Apr. 15, 1994).

commitment schedule and additionally apply to all "transport of electronic signals."[51] While there are specific restrictions for EU member states, there are no references to privacy protections, data localization requirements, or cyber-security.[52] One notable exception, however, is noted in the most recent revision, which specifies some restrictions on transfers for "financial data processing."[53]

However, because the EU has gone out of its way to specifically carve out financial data processing services, one can infer that the current schedule of commitments includes all other digital transfers not within the financial services carve out.[54] While some might be inclined to argue that the "standstill" provision should be used here to defend the EU's commitments because of their age, this argument holds little water.[55] That is because the EU Data Protection Directive (DPD) was adopted in 1995, between the time of the initial commitment and the revision.[56] Thus, it seems likely that the EU had at least a fundamental understanding of the treatment of citizen's data and personally identifiable information through digital transfers. Additionally, because the EU has not altered its commitments after passing the GDPR,[57] which directly updates the EU DPD, it is reasonable to argue that the current commitments should be interpreted broadly to include all data transfers with the single exception of financial services.[58]

B. *China*

China's commitments to the GATS are much more nuanced, specific, and restrictive than the EU or Russia.[59] While there are no restrictions or exemptions under Mode 1 for computer data processing

51. *European Communities and Their Member States - Schedule of Specific Commitments: Supplement 3*, 1-3, WTO Doc. GATS/SC/31/Suppl.3 (Apr. 11, 1997).

52. *See id.*

53. *European Communities and Their Member States - Schedule of Specific Commitments: Supplement 4*, 9, WTO Doc. GATS/SC/31/Suppl.4/Rev.1 (Nov. 18, 1999).

54. *Id.*

55. GATS Handbook, *supra* note 30, at 20-21.

56. Council Directive 95/46 of 24 Oct. 1995, (L 281/31), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=bg.

57. *See generally* Council Regulation 5419/16 of 6 Apr. 2016, Preamble, http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf [hereinafter GDPR].

58. *European Communities and Their Member States - Schedule of Specific Commitments: Supplement 4*, 9, WTO Doc. GATS/SC/31/Suppl.4/Rev.1 (Nov. 18, 1999).

59. *See generally People's Republic of China - Schedule of Specific Commitments*, WTO Doc. GATS/SC/135 (Feb. 14, 2002).

services,[60] telecommunications service providers are included in a list of Mode 3 exemptions which require foreign service suppliers to establish joint venture enterprises limited to specific cities with no more than fifty percent ownership.[61] Thus, China's localization and screening rules have been somewhat cemented in their GATS commitments, at least with regard to telecommunications transfer services, but other services facilitated through digital transfers, like data processing, remain far less limited.[62] Because this Note analyzes Mode 1 transfer, specifically, and because telecommunications service providers only render a final delivery of digital transfers services, we can reasonably assume that China's commitments would cover a significant volume of data transfers services from the United States.

C. *Russia*[63]

Because its commitments were made in 2012, Russia cannot make a sound argument that it did not fully comprehend the nature of international data flows when it made its commitments, as the Internet of 2012 was far more sophisticated and globalized than in 1994.[64] Russia's commitments specifically cover electronic mail, voice mail, online information and database retrieval, electronic data interchange, and other related data transfers.[65] The only limitations provided for market access and national treatment, with respect to Mode 1, are for radio and satellite communications providers, operators of which are required to have a licensed juridical person residing in the Russian Federation.[66] Russia also made further commitments, negotiated as part of its accession; these commitments include transparency for licensing, as well as provisions to ensure equal and fair treatment for "interconnection."[67] Interestingly, there are no references in any of these documents to privacy, cybersecurity, or localization.[68] Thus, Russia's commitments are

60. *Id.* at 9-10.

61. *Id.* at 17.

62. *See id.*

63. In part because it is one of the most recent Members to join the WTO, Russia's commitments are all located in a single document without further revisions. *See generally Russian Federation - Schedule of Specific Commitments*, WTO. Doc. GATS/SC/149 (Nov. 5, 2012).

64. *Id.*

65. *Id.* at 25-26.

66. *Id.*

67. Working Party on the Accession of the Russian Federation, *Report of the Working Party on the Accession of the Russian Federation*, WTO Doc. WT/ACC/RUS/70/Add.2 (Nov. 17, 2011).

68. *See id.*

not only the broadest of the three WTO members, but also more timely and technologically inclusive.

D. *Progress Report on Electronic Commerce 19 July 1999*

Outside of the specific WTO member commitments and the actual GATS agreement, other reports from the WTO provide informative context. In July 1999, the Work Programme on Electronic Commerce produced a progress report to the General Council outlining the relationship between the GATS and electronic delivery of services.[69] That report explains the general view that "electronic delivery of services falls within the scope of GATS," and that the GATS is "technologically neutral."[70] The group also found it difficult to distinguish between Modes 1 and 2 for purposes of e-commerce, with no conclusion on how to clarify the issue.[71] This lack of clarity is a significant issue in the analysis of the EU, Russia, and China's data transfers laws because there was no distinction on the individual schedules for telecommunications or data processing exemptions between transfers made via Modes 1 or 2.

The report continues by analyzing member views on Articles VI, XVI, and XVII, but the comments on Article XIV—discussed further in this section—are perhaps the most key, as they describe the members views on the privacy, public morals, and prevention of fraud exceptions; there was agreement, however, that whatever regulations the members used to exercise their rights under Article XIV, they must not "constitute a means of arbitrary or unjustifiable discrimination, or disguised restriction on trade in services."[72] Furthermore, the report agreed that Article XIV should be interpreted "narrowly."[73] With regard to Article XVI, the report found there was disagreement between members on whether scheduled commitments on basic telecommunications services covered the full range of all Internet services, or if the specific services would need to be scheduled as well.[74] In short, despite some disagreement on specific interpretation and an emphasis on Article XIV privacy

69. Work Programme on Electronic Commerce, *Progress Report to the General Council*, WTO Doc. S/L/74 (Jul. 27, 1999).

70. *Id.* at 1 (noting also some members' views that the issues were "complex and needed further examination").

71. *Id.*

72. *Id.* at 2-4.

73. *Id.* at 4.

74. *Id.* Note: because there are dozens of other services that can be targeted by one member against another for purposes of this paper, it is assumed that even if a broad interpretation of basic telecommunications commitments is not sufficient, there are enough more industry specific commitments that could be pulled in to enhance the argument.

protections, the WTO electronic commerce progress report from nearly two decades ago indicates close agreement between members on the importance of broad interpretation of GATS provisions to facilitate electronic data transfers and commerce.[75] As time has passed, the WTO has not changed or altered these assumptions; therefore, it is reasonable to assume that these same views are still held today.

V. Arguments for Data Restrictions: National Security and Human Rights

While protection of personal information has been enshrined as a human right for decades,[76] the advent of the Internet, servers, smartphones, and other electronic transfer devices and techniques has, in the view of many, expanded the scope of potential damage to individuals.[77] Millions of Americans, for example had their private information stolen due to a security breach at Equifax,[78] as well as similar breaches at Yahoo and Uber.[79] These breaches have led to lawsuits and even to calls for judicial dissolution,[80] and these are just three of countless other breaches that have already been disclosed to public.[81] Companies

75. *See id.*

76. The right to privacy is explicitly named in the Universal Declaration of Human Rights (art. 12), International Covenant on Civil and Political Rights (art. 17), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (art. 8). *See, e.g.*, Universal Declaration of Human Rights, G.A. Res. 217A, U.N. GAOR, U.N. Doc A/810, art. 12 (Dec. 12, 1948), http://www.un.org/en/universal-declaration-human-rights/; International Covenant on Civil and Political Rights, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. art. 17 (entered into force Mar. 23, 1976); European Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Nov. 4, 1950, 213 U.N.T.S. art. 8 (entered into force Sept. 3, 1953).

77. For a brief history in the context of the OECD, *see generally* Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, OECD Digital Econ. Papers No. 187, 15 (2011), http://www.kuner.com/my-publications-and-writing/untitled/kuner-oecd-tbdf-paper.pdf.

78. Seena Gressin, *The Equifax Data Breach: What to Do*, Fed. Trade Commission (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

79. *Id.*

Elizabeth Weise, *Yahoo says 2013 hack hit all 3 billion user accounts, triple initial estimates*, USA Today (Oct. 3, 2017), https://www.usatoday.com/story/tech/2017/10/03/3-billion-yahoo-users-breached-company-says/729155001/; Mike Isaac, Katie Benner & Sheera Frenkel, *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. Times (Nov. 21, 2017) https://www.nytimes.com/2017/11/21/technology/uber-hack.html.

80. Ron Fein, *Equifax Deserves the Corporate Death Penalty*, Wired (Oct. 20, 2017), https://www.wired.com/story/equifax-deserves-the-corporate-death-penalty/.

81. *See, e.g.*, Lewis Morgan, *List of data breaches and cyber attacks in October 2017 – 55 million records leaked*, IT Governance (Oct. 30, 2017), https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-october-2017-55-million-records-leaked/.

are deeply concerned about protecting their information from theft or discovery, and make massive time and resource investments in an effort to do so.[82] Furthermore, while there is great concern by consumers about their data being expropriated by governments, this is another issue entirely.[83] Instead, this Note will narrowly focus on laws and regulations that seek to protect consumers from the exposure of their data, with a particular emphasis on the EU's GDPR law that will go into effect in May 2018.[84]

A major issue is that governments are still working to move their laws into the twenty-first century when it comes to regulating privacy, consumer protections, and requirements for storing and transferring data.[85] Some governments have responded by filtering and blocking access to online content.[86] Others have been more sophisticated in their approaches, such as with the EU's GDPR law.[87] There has also been pressure to include in new and recent trade agreements, such as the Trans-Pacific Partnership ("TPP"), EU-Canada Comprehensive Economic and Trade Agreement ("CETA"), and the North American Free Trade Agreement ("NAFTA") 2.0, language that prohibits or restricts mandatory localization of data.[88] However, countries that prioritize privacy and consumer protections have pushed back and demanded data localization or restrictions on incoming and outgoing data transfers on the basis that such regulations and restrictions improve commercial privacy and data security.[89] More recently, there

82. *See, e.g.*, Brian Barrett, *Breaking Down HBO's Brutal Month of Hacks*, WIRED (Aug. 18, 2017), https://www.wired.com/story/hbo-hacks-game-of-thrones/ (explaining that HBO had their servers hacked, on multiple occasions, that culminated with a Game of Thrones episode posted online before it had actually aired).

83. Ashley Gorski & Scarlet Kim, *Why do we still accept that governments collect and snoop on our data?*, THE GUARDIAN (Oct. 30, 2016), https://www.theguardian.com/commentisfree/2016/oct/30/government-data-collection-citizens-acceptance-global-rights-privacy-free-speech.

84. *Id. See generally* GDPR, *supra* note 57; *see also* Laura Hautala, *Equifax hack may shake up US consumer data laws*, CNET (Oct. 20, 2017), https://www.cnet.com/news/equifax-hack-may-shake-up-consumer-data-laws/ (arguing that a potential U.S. law should could come into being that might violate these same rules).

85. EU GDPR is a great example of this shift, as the EU has passed into law a comprehensive privacy bill that updates the much older Data Protection Directive from the 1990's. *See* GDPR, *supra* note 57.

86. Sanja Kelly et al., *Silencing the Messenger: Communications Apps Under Pressure*, FREEDOM HOUSE (2016), https://freedomhouse.org/report/freedom-net/freedom-net-2016.

87. *See, e.g.*, analysis *infra* of the EU's laws in contrast to the laws in China.

88. Nigel Cory, *Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?*, INFO. TECH. & INNOVATION FOUND. 2-3 (May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf.

89. *Id.* at 3.

has been a backlash against these claims, with opponents arguing that these rules cause more problems than they solve.[90]

This backlash is owed to the fact that many privacy laws, including localization requirements, often create less secure systems and processes that leave citizens more vulnerable, whether it be from private actors or host governments.[91] Some opponents have also argued that localization requirements are simply unnecessary to protect privacy, making these localization laws fundamental trade barriers without de facto purpose and in clear violation of the GATS.[92] The problem is that depending on how a state implements its laws, localization requirements can serve other purposes, and some of the named purposes have caused hesitation by countries concerned with terrorism and other national security threats to engage in these issues at the WTO.[93]

Perhaps the biggest hurdles in bringing and winning a case before the WTO are the GATS Article XIV exceptions, one of which specifically protects laws and regulations created to protect the "privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[94] So long as the "measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or disguised restriction on trade in services," these measures are protected under the GATS.[95] Furthermore, for countries who argue that their localization requirements are necessary to ensure security and protections for

90. *See, e.g.*, Daniel Castro, *The False Promise of Data Nationalism*, INFO. TECH. & INNOVATION FOUND. (May 2017), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

91. *See* Holly Dragoo, *New Russian Law Mirrors China in Restricting Use of VPNs*, GA. TECH., https://iisp.gatech.edu/new-russian-law-mirrors-china-restricting-use-vpns (arguing the China and Russia have employed localization requirements with anti-VPN laws to restrict access to uncensored content websites such as Facebook, Wikipedia, and Reddit). As one example of this, many Canadians argue that the provincial localization requirements in British Columbia bolster privacy, yet those same laws may actually make data more vulnerable due to lower-quality encryption, servers, and physical access; these issues are often exaggerated in other countries like Russia. *See* Courtney M. Bowman, *A Primer on Russia's New Data Localization Law*, PRIVACY L. BLOG (Aug. 27, 2015), http://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/.

92. *See, e.g.*, Castro, *supra* note 90.

93. *Compare* Catherine Stuff, *European Commission Paralysed Over Data Flows in TiSA Trade Deal*, EURACTIV (Oct. 11, 2016), https://www.euractiv.com/section/trade-society/news/european-commission-paralysed-over-data-flows-in-tisa-trade-deal/ *with* Jeremy Malcom, *TISA Proposes New Global Rules on Data Flows and Safe Harbors*, ELECTRONIC FRONTIER FOUND. (Oct. 24, 2016), https://www.eff.org/deeplinks/2016/10/tisa-proposes-new-global-rules-data-flows-and-safe-harbors.

94. General Agreement on Trade in Services, Apr. 15, 1994, 1869 U.N.T.S. 183.

95. *Id.*

their citizens Article XIV *bis* stands as another hurdle.[96] Several authors have argued, however, that these exceptions are not sufficient to protect the EU's older law, the Data Protection Directive ("DPD").[97] This Note extrapolates on those arguments, analyzes the broader context of localization and privacy protections, and finds that such laws could very likely be challenged before the WTO. Furthermore, the Note also asserts that these claims could be made without interfering with the national security arguments implemented in the context of other unrelated laws, regulations, and policies.

VI. Defining Privacy Protections and Confidentiality

Because of the broad territorial reach, fines, and stringent rules of the EU's new privacy law, there will likely be new motivation for data transfer companies to raise the idea of a WTO suit with their host governments when the GDPR is implemented in May 2018.[98] In an attempt to preempt these attacks, some officials in the EU, such as Former Justice Commissioner and MEP Viviane Reding, have warned, "Data protection is no trade barrier, it is a fundamental right."[99] Before analyzing the EU's GDPR, though, it is first important to recognize the fundamental principles of data transfer, which typically begins with an analysis of controllers and processors.[100]

The distinction between who controls and who processes data is a prominent feature of the laws in the EU and has been expounded in the EU's GDPR and further clarified by the controlling Data Protection Authorities ("DPAs").[101] Per those definitions, a "controller" is the natural or legal person, organization, government, or any other body that determines the "purposes and means of processing personal data."[102]

---

96. *Id.*

97. *See, e.g.*, Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 Stan. L. Rev. 1315, 1334-39 (2000) (describing country to country variations of the DPD).

98. *See generally* GDPR, *supra* note 57.

99. Monika Ermert, *EU Parliament Hearing: Data Protection not a Trade Barrier, but a Fundamental Right*, Intellectual Property Watch (June 18, 2015), https://www.ip-watch.org/2015/06/18/eu-parliament-hearing-data-protection-not-trade-barrier-but-fundamental-right.

100. *See Are You a "Data Controller"?*, Data Protection Commissioner - Ireland, https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm.

101. *See, e.g.*, *Data Controllers and Data Processors: What the Difference is and What the Governance Implications Are*, ICO, https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

102. GDPR art. 4(7); for a summary of important definitions and a brief comparison between the definitions in the DPD and GDPR, *see* Detlev Gabel & Tim Hickman, *Chapter 5: Key Definitions–Unlocking the EU General Data Protection Regulation*, White & Case (Sep. 13, 2017), https://www.

According to Article 4(8) of the GDPR, a "processor" is an entity that processes personal data for or on behalf of a controller.[103] As the data age has progressed, a new designation for "sub-processors" has also been created to provide direction to organizations that handle data given to them from a processor who received that same information from the original data controller.[104] This construction is important to understand because the essential idea behind the GDPR was to create a law that would ensure privacy and data security protections for EU residents no matter who controlled, processed, or facilitated use of personally identifiable information.[105]

An important issue to remember, however, is that the EU body only has the authority to regulate commerce, both foreign and domestic.[106] It does not, however, have the authority to control national security legislation or agenda of member states.[107] In part to curtail the restrictive national security arguments for localizing data and restricting internal data transfers between fellow EU Member States, the EU launched the Digital Single Market (DSM) initiative in May 2015.[108] Throughout this process, however, pushback from France and Germany,[109] as well as

whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation.

103. GDPR art. 4(8). *See also* Detlev Gabel & Tim Hickman, *Chapter 11: Obligations of Processors–Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Jul. 22, 2016), https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection (comparing to the DPD and highlighting the potential impact of this change).

104. GDPR art. 28(2),(4). *See also* Gabel & Hickman, *supra* note 103 (alluding to the idea that theoretically, this chain of processor/sub-processors can continue into perpetuity).

105. *See, e.g.*, GDPR, *supra* note 57, preamble. *See also id.*

106. *See, e.g.*, Joshua Rozenberg, *Does the EU Impact on UK Sovereignty?*, BBC (Feb. 23, 2016), http://www.bbc.com/news/uk-politics-eu-referendum-35630757 (discussing the limits of EU's authority and impact on the UK's sovereignty). *See also* Derrick Wyatt, *How the EU Works: the EU's Powers*, FULL FACT (Apr. 14, 2016), https://fullfact.org/europe/eus-powers/.

107. *See, e.g.*, Henry Farrell, *Here's Why Europe Can't Police Terrorism Very Well*, WASHINGTON POST (Mar. 22, 2016), https://www.washingtonpost.com/news/monkey-cage/wp/2016/03/22/heres-why-europe-cant-police-terrorism-very-well/?utm_term=.478c1e763f98.

108. *Shaping the Digital Single Market*, DIGITAL SINGLE MARKET, https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market (last visited May 1, 2018).

109. Though France ultimately rejected a proposed localization amendment, the debate has not ended. *French Parliament Rejects Data Localization Amendment*, HUNTON & WILLIAMS (Jul. 1, 2016), https://www.huntonprivacyblog.com/2016/07/01/french-parliament-rejects-data-localization-amendment. Currently the Telecommunications Act in Germany requires that telecommunications providers store metadata within Germany for a specified period of time. *See Data Localization Snapshot*, ITI (Jan. 19, 2017), https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf). Additionally, Chancellor Merkel previously backed a proposal for "European data networks that would keep emails and other communications on the European side of the Atlantic." Alison Smale, *Merkel Backs Plan to Keep European Data in Europe*, N.Y. TIMES

other member states, against the United States' national security collection techniques has resulted in an ongoing debate about a Europe-only cloud. Thus, while several EU members have localization laws—including many that have been targeted by USTR as restrictive to data transfers—these laws are not EU-wide and may be overturned via the DSM initiative.[110] Therefore, this Note will focus primarily on the cybersecurity and privacy protections in the EU broadly and not on the individual requirements of each member-state.

VII. The Crux: GATS Article XIV(c)(ii) – Exception for Privacy Protections

A specific definition of privacy protections is critical because the GATS agreement itself provides an important exception to member states who, in pursuit of citizen privacy, would otherwise violate their GATS obligations. As a shield against claims against their privacy laws, WTO members can claim adherence to the Article XIV(c)(ii) exception.[111] That provision asserts that member states may violate their other GATS commitments if they do so in a way that is "necessary to secure compliance with laws or regulations" that provide "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[112] While no case has been raised where GATS Article XIV(c)(ii) has been effectively used as a defense, the Appellate Body ruled in *Argentina-Financial Services* (2016)[113] that for a measure to be justified generally under Article XIV(c), the respondent must show that 1) the measure was designed to secure compliance with laws or regulation that are not themselves inconsistent with the GATS; and 2) "the measure must be necessary to secure such compliance."[114]

(Feb. 16, 2014), https://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html. *See also* Ben Knight, *German Data Storage Laws "Threaten Free Trade,"* Deutsche Welle (Jan. 12, 2017), http://www.dw.com/en/german-data-storage-laws-threaten-free-trade/a-37110699.

110. Off. of the U.S. Trade Rep., 2017 National Trade Estimate Report on Foreign Trade Barriers, 178-81 (2017).

111. GATS art. XIV(c)(ii).

112. *Id.*

113. Appellate Body Report, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, ¶ 157, WTO Doc. WT/DS161/AB/R (adopted Dec. 11, 2000) (regarding the Article XX(d) exception of the GATT 1994).

114. Appellate Body Report, *Argentina – Measures Relating to Trade in Goods and Services*, ¶ 6.202, WTO Doc. WT/DS453/AB/R (adopted Apr. 14, 2016). *See also, generally*, Peter Van den Bossche & Werner Zdouc, The Law and Policy of the World Trade Organization (4th ed. 2017).

Thus, for a privacy law to be properly covered under this exception, it must have a precise definition of privacy and provide a limited restriction—or set of restrictions—that is necessary to achieve the intended protection. This means that whatever law is implemented must be shown to actually enhance the privacy protections and in the best or only way possible.[115] Because this two-pronged test would theoretically force any nation that seeks to use it to walk a proverbial tightrope, there has likely been some trepidation on the part of member states in bringing a suit against another member state that is likely to assert an Article XIV(c) defense.[116] By including privacy provisions only if they are necessary for both the protection from "processing and dissemination" as well as the "protection of confidentiality" of personal information, member states are forced to both defend the sacrosanct nature of privacy against foreign bodies, nations, and companies, while also explaining why the member state of origin can provide the protection necessary and other member state cannot.[117] Because this comparison between countries will be a priority consideration of any WTO panel, this Note accepts the premise that the United States provides more protections for consumers and citizens than either Russia[118] or China,[119] and that the EU and the United States provide, at least arguably, "essentially equivalent" protections for consumers.[120] While obviously a fiercely debated issue, there are sound and reasoned arguments that the United States can take into account the various laws and national security regimes[121] of each individual member-state in the EU

115. Arguably, it is for this reason that the EU has begun to pull away, in some respects, from the idea of a Europe-only cloud.

116. Appellate Body Report, *supra* note 114, ¶ 6.202.

117. This has given rise to an enormous body of literature and argument, including Sidley Austin's *Essentially Equivalent* treatise. Jacques Bourgeois et al., *Essentially Equivalent*, DATAMATTERS. SIDLEY.COM (Jan. 2016), https://www.sidley.com/-/media/publications/essentially-equivalent—final.pdf?la=en.

118. Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet*, EMORY L. J. (forthcoming) (citing Alexandra Kulikova, *Data Collection and Retention in Russia: Going Beyond the Privacy and Security Debate*, GLOBAL PARTNERS (Jan. 17, 2014), http://www.gp-digital.org/gpdupdate/data-collection-and-retention-in-russia (noting the FSB's direct access to mandatorily localized data for terrorism purposes without a court order)).

119. *Id.* at 8-9.

120. Bourgeois et al., *supra* note 117.

121. *See* Patrick S. Ryan et al., *When the Cloud Goes Local: The Global Problem with Data Localization*, 46 COMPUTER 54, 58 (2013) (citing Doug Longhini, *We'll Be Listening: Amanda Knox Case Reveals Extent of Italian Wiretapping*, CBS NEWS, (Nov. 23, 2011), https://www.cbsnews.com/news/well-be-listening-amanda-knox-case-reveals-extent-of-italian-wiretapping). *See generally* WINSTON MAXWELL & CHRISTOPHER WOLF, A GLOBAL REALITY: GOVERNMENTAL ACCESS TO DATA IN THE CLOUD, (2012), http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_

in a way that would at least raise doubt against the necessity and precision of EU laws and regulations.[122] In order to fully explain this argument, however, a deeper inspection of the EU's privacy program, its purposes, and methods is warranted.

VIII. GDPR, Localization Proposals and Tension Between the EU and Its Members

Brexit is, perhaps, the best illustration of the heightened tension between the EU and the individual members of the union.[123] This tension, and the limited overlapping powers with regard to national security, trade, and international commerce contribute to the argument that the United States and EU provide essentially equivalent protections for data. Such an argument is enhanced by the fact that the EU specifically created a series of programs, laws, and regulations that allow data transfers from the EU to the United States based merely on contractual language and its subsequent enforceability in U.S. courts and before U.S. regulators.[124] This specific enhancement of the "essentially equivalent" argument is important because it demonstrates that the EU does have at least limited trust in the privacy protections granted in the United States—protections that are provided in a totally different way and with far fewer restrictions on international transfers.[125] Additionally, as discussed below, EU officials have tipped their hands when it comes to the "necessity" of EU laws and regulations to protect privacy.[126] Any arguments the EU might make about the necessity of its laws is furthered by the widely varying and colorful tapestry of different localization laws in each of the individual member states.[127]

Cloud_Data_Paper_1_.pdf; Jane McCallion, *Report: "European Clouds Are Not Safe from Government Snoopers"*, CloudPro (May 24, 2012), http://www.cloudpro.co.uk/cloud-essentials/3737/report-european-clouds-are-not-safe-government-snoopers.

122. This side of the debate is taken not only because it enjoys a widespread academic following, but also because the position need only be reasoned, logical, and grounded to get traction before the WTO in this context. As noted above, it need not be wholly correct, but rather correct enough to cast doubt that the EU's laws and regulations are absolutely necessary to ensure the warranted protections.

123. *See, e.g.*, Rozenberg, *supra* note 106 (discussing the limits of the EU's authority and impact on the UK's sovereignty).

124. Model contracts, Binding Corporate Rules, and the Privacy Shield program essentially operate under the premise that contractual clauses are enforceable in the U.S. and will provide EU consumers with the necessary protections.

125. Bourgeois et al., *supra* note 117.

126. *See generally* Svetlana Yakovleva & Kristina Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, 2 Eur. Data Protection L. Rev. 191 (2016).

127. *Id.*

A. *Introduction*

The EU continues to be viewed as the leader on privacy standards, and with the EU's global reach and impact, it has created a type of privacy "hegemony."[128] It is home to some of the most powerful data protection authorities (quasi-governmental bodies that regulate, fine, and censure organizations).[129] Furthermore, the EU's GDPR law contains detailed descriptions, definitions, regulations, and treatment for many types of data transfers, retention systems, and processing.[130] These details are, in part, because the EU is concerned that companies and nations will transfer data out of the EU to another jurisdiction with different rules and fail to provide adequate protections.[131]

Not only does the EU set itself up as an example to other nations on privacy protections, but it also requires that other countries provide "adequate" protections before data can be transferred to those jurisdictions.[132] Not including the three EEA members and United States (with an appropriate transfer mechanism, like Privacy Shield), the EU has only found 11 other countries to provide adequate protections for citizens' data.[133] Thus, though the EU may be seen as the leader by many, in privacy protections, it has not been followed well enough for the EU Commission and Parliament to grant open data transfers between the EU and those other countries.

B. *Initial Concern About GATS Violations from Within the EU*

As noted above, for a country to demonstrate that a barrier is legitimate under an Article XIV exception, it must show that the law is necessary. Because the EU continues to change its rules, regulations, and policies on data transfers so frequently, the bloc may now be on shaky ground, and some of its leaders appear to realize this.[134] In fact, two

128. *See generally* Graham Greenleaf, *International Data Privacy Agreements After the GDPR and Schrems*, 139 PRIVACY LAWS & BUS. INT'L REP. 12 (2016).

129. Jason Weinstein, *The U.S. Doesn't Have a National Data Protection Authority? Think Again . . .* , IAPP (Oct. 16, 2013), https://iapp.org/news/a/america-doesnt-have-a-national-data-protection-authority-think-again/#.

130. *See, e.g.*, GDPR, *supra* note 57, art. 28 (regulating actions taken by processors).

131. *Compare* Stuff, *supra* note 93 *with* Malcom, *supra* note 93.

132. *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

133. *Id.*

134. Viviane Reding & Jan Philipp Albrecht, *Don't Trade Away Data Protection*, POLITICO (Mar. 30, 2017), https://www.politico.eu/pro/opinion-dont-trade-away-data-protection.

leading members of the EU Parliament have specifically called for a repeal of the necessity and consistency tests in GATS Article XIV.[135] This may be, in part, why the EU has turned to the broad extraterritoriality provisions in the GDPR to push consumer protections.[136] Broad extraterritoriality provisions force foreign-based companies to operate by the same standards as domestic companies, both staring down the barrel of up to four percent of global, top-line revenue fines for noncompliance.[137] These fines and the relative benefit provided to EU organizations that have become accustomed to the EU's route and means of protecting privacy make for a strong argument that the EU is providing a regulatory leg-up to domestic service and data flows providers. The fact that leaders in the EU are asking for a fundamental change to the GATS should cause concern.[138] It is one thing to argue that a law is compliant with WTO commitments, but quite another to accept there may be an issue, pass the law anyway, and then try to remedy the situation by requesting a fundamental change to GATS Article XIV exception. Thus, the arguments made by these EU officials should prove instrumental to any complaint brought before the WTO by the United States against the EU.

C. *Localization Proposals in the EU*

Following the Snowden revelations,[139] several countries, including Germany and France, have proposed a sort of "Schengen cloud" or "Schengen internet" that would localize information in the EU.[140] The idea is that by retaining all information on locally-based servers, EU citizens will not need to fear foreign governments' data collection programs.[141] As one author convincingly argued, however, there is a "false promise" in the arguments for "data nationalism," and if the EU were to continue down this path of localization, it would be even harder for

135. *Id*; *see also* Carl, *Trade Agreements and Data Protection: Changing GATS Article XIV Is Not the Way to Go*, SIIA (Apr. 13, 2017), https://www.siia.net/blog/index/Post/71796/Trade-Agreements-and-Data-Protection-Changing-GATS-Article-XIV-is-Not-the-Way-to-Go.

136. *See generally* GDPR, *supra* note 57.

137. *Id.*, art. 28.

138. Stuff, *supra* note 93; Malcom, *supra* note 93. *But see* Carl, *supra* note 135.

139. *See, e.g.*, Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded*, THE GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (a much more detailed history of the Snowden revelations).

140. W. Kuan Hon, *Policy, Legal and Regulatory Implications of a Europe-Only Cloud*, 24 INT'L J. L. INFO. TECH. 251, 251-53 (2016); *see also* Ryan et al., *supra* note 121, at 57.

141. Hon, *supra* note 140, 251-53.

them to argue that their requirements are both necessary and consistent as required by GATS Article XIV.[142] Another author explains that while the Snowden revelations understandably shook the EU, so-called "Balkanization" or mandatory localization, would not actually improve privacy and only threatens the lawfulness of the GDPR.[143] Thus, while there has been some talk of localization among member states, the EU will be keen to push back against these proposals. If, however, such a policy is passed, the United States should immediately greenlight a WTO challenge as the conflicts between the GDPR and specific localization laws will put both laws and regulations in peril in the eyes of the WTO. Because no such laws have taken effect, this paper assumes that the EU will be able to constrain its members.

D. *The EU as the Trade Negotiating Body*

There is unavoidable tension surrounding the EU data rules however, because while many member states are calling for localization, recent statements from the European Commission assert that the extraterritorial reach of the GDPR obviates the need for localization requirements.[144] In fact, according to a recent statement, the EC wants to end forced localization, period.[145] The problem is that the EU does not have total authority over its member states in all of their activities.[146] Importantly, the EU has very limited authority over controlling individual member-state national security regimes.[147] While there has long been tension between national security and privacy,[148] this issue has

142. Castro, *supra* note 90.

143. Hon, *supra* note 140, 251-53.

144. Sam Pfeifle, *Is the GDPR a Data Localization Law?*, IAPP (Sept. 29, 2017), https://iapp.org/news/a/is-the-gdpr-a-data-localization-law.

145. Jennifer Baker, *EU Commission Aims to Ban Forced Data Localization*, IAPP (Oct. 24, 2016), https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization/; Jennifer Baker, *European Commission Eyes an End to Data Localization in EU*, IAPP (Jan. 12, 2017), https://iapp.org/news/a/european-commission-eyes-an-end-to-data-localization-in-eu/.

146. *See, e.g.*, Rozenberg, *supra* note 106 (discussing the limits of EU's authority and impact on the UK's sovereignty); *see also* Wyatt, *supra* note 106.

147. Stratfor Enterprises, LLC., *The European Union Is Not a Security Union*, STRATFOR (Mar. 25, 2016), https://worldview.stratfor.com/article/european-union-not-security-union.

148. *See, e.g.*, Benjamin Wittes, *What Ben Franklin Really Said*, LAWFARE (July 15, 2011), https://www.lawfareblog.com/what-ben-franklin-really-said#.UvvR12RDtZs (quoting Benjamin Franklin "Those who would give up essential Liberty to purchase a little temporary Safety, deserve neither Liberty nor Safety"). *See also* Lee Rainie & Shiva Maniam, *Americans feel the tension between privacy and security concerns*, PEW RES. CTR. (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ (highlighting current polling on American views of privacy vs. security).

been exacerbated by the rift between consumer protections at the EU level and member-state national security protections at the member level.[149] However, because there has not been a ruling issued by the WTO on a complaint involving a GATS Article XIV defense for privacy laws, it is impossible to know how the WTO will weigh such a discrepancy. The concerns and arguments for altering the GATS, however, make much more sense in this context, and this discrepancy should remain a great concern for the EU, as the national security laws may very well conflict with each other as well as some of the purposes and intentions of the GDPR. While a harder, more uphill battle than that against Russia and China (as discussed in Part VIII), a WTO case against the EU would nevertheless be the most likely to shatter privacy restriction arguments globally, due in part to the reality that the EU, in relation to most other WTO members, has perhaps the longest track record of legislating privacy protections.

IX. Political Suppression: The Inverted Privacy Argument (Russia and China)

The contradiction of localization requirements and privacy rules might be causing debate in the EU right now, but this contradiction has been all but ignored elsewhere. Two stark examples of this ignorance elsewhere are the localization and cybersecurity laws in Russia and China. In fact, the privacy and data "protections" in China and Russia have been flagged as double-edged swords by many human-rights watchdogs.[150] Both countries have enacted laws that allege protections for citizens,[151] but, as many argue, the laws only act as a means for suppression and surveillance.[152] Furthermore, as cited in a 2017 report by the Information Technology Industry Council (ITI), these

149. Christopher Wolf & Winston Maxwell, *Why the U.S. Is Held to a Higher Data Protection Standard Than France*, IAPP (Nov. 2, 2015), https://iapp.org/news/a/why-the-u-s-is-held-to-a-higher-data-protection-standard-than-france/ (arguing that France's mass surveillance regime threatens European privacy more than U.S. laws do).

150. *See, e.g.*, Jyoti Panday, *Rising Demands for Data Localization a Response to Weak Data Protection Mechanisms*, EFF 3 (Aug. 14, 2017), https://www.eff.org/deeplinks/2017/08/rising-demands-data-localization-response-weak-data-protection-mechanisms.

151. Derek Luke, *Data Localization Laws: an Emerging Global Trend*, Jurist 1-2 (Jan. 6, 2017), http://www.jurist.org/hotline/2017/01/Courtney-Bowman-data-localization.php.

152. *See e.g.*, Andrei Soldatov, *Putin Has Finally Reincarnated the KGB*, Foreign Pol'y 1 (Sept. 21, 2016), http://foreignpolicy.com/2016/09/21/putin-has-finally-reincarnated-the-kgb-mgb-fsb-russia/.

laws create clear barriers against digital trade.[153]

A. *Localization for Citizen "Privacy": Russia*

In December 2014, President Putin signed Russia's personal data localization law that mandates data controllers "record, systemize, accumulate, store, amend, update and retrieve"[154] data from local systems in Russia.[155] This law has allowed Russia to mandate that companies like Facebook, Apple, and Google store data locally on servers in Russia; otherwise the companies will face an access block.[156] While some companies, like Apple, quickly complied with the law, others, like Google, Facebook, and Twitter contemplated their options for a much longer period.[157] Much of this hesitation is likely because of the costs associated with localization, but equally important, Russia's localization rules have been perceived as "part and parcel of a comprehensive crackdown on political dissent and the perceived threat of foreign meddling in Russia's domestic politics."[158]

These crackdown tactics are possible because, so long as the data is localized, the Federal Security Service ("FSB")—the successor to the KGB—is able to define interception procedures in a way that has allowed them to access locally stored data without a warrant or court

153. *See generally Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses*, ITI, https://www.itic.org/dotAsset/9/d/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf (last visited Dec. 18, 2017).

154. Duane Morris LLP, *Russia's Personal Data Localization Law: Expanding Enforcement*, MARTINDALE HUBBARD 1 (Aug. 2, 2016), https://www.martindale.com/internet-law/article_Duane-Morris-LLP_2232152.htm. *See also*, Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, BNA (Aug. 10, 2015), https://www.bna.com/russia-clarifies-looming-n17179934521/ (interpreting the Russian ministry's clarifications of the new law).

155. *Id.*; *See also* Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, BNA (Aug. 10, 2015), https://www.bna.com/russia-clarifies-looming-n17179934521/ (interpreting the Russian ministry's clarifications of the new law); *3 Things To Know About Russia's New Data Localization Law*, LAW360 (Sept. 3, 2015), https://www.law360.com/articles/698895/3-things-to-know-about-russia-s-new-data-localization-law.

156. Dmitry Solovyov, *Russia tells Facebook to localize user data or be blocked*, REUTERS (Sept. 26, 2017 ed. Andrew Osborn), https://www.reuters.com/article/us-russia-facebook/russia-tells-facebook-to-localize-user-data-or-be-blocked-idUSKCN1C11R5.

157. Peter Judge, Russian Data Law: Apple Complies, Google and Facebook Delay, DATA CTR. DYNAMICS (Sept. 14, 2015), http://www.datacenterdynamics.com/content-tracks/design-build/russian-data-law-apple-complies-google-and-facebook-delay/94785.fullarticle.

158. *Data Localization: A Challenge To Global Commerce and the Free Flow of Information*, ALBRIGHT STONEBRIDGE GROUP 9 (Sept. 2015), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf.

order.[159] According to the Russian Supreme Court, the FSB has massively ramped up its eavesdropping on Russian citizens alone.[160] The new laws and broad authority granted to the FSB have led some to argue that KGB agents would actually be jealous of the FSB's power, authority, and eavesdropping capabilities today.[161]

Interestingly, Russia also provides a limited list of authorized countries that can receive data transfers from Russia because those countries provide sufficient privacy protections.[162] It should be noted that neither the United States nor the EU are included in this list, though Israel, New Zealand, and some other countries listed on the EU's adequacy list are.[163] The existence and purpose of this list should be scrutinized, however, as Roskomnadzor, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Russia's data protection authority) is not only supposed to determine how to best protect consumer privacy, but it has also played a key role in enforcing the new localization law against companies like Facebook.[164] In the end, it would likely be very difficult for Russia to argue its localization rules are both necessary and consistent under GATS Article XIV.

B. *Cybersecurity Restrictions to Keep Citizens "Safe": China*

China has been combating free trade arguments against mandatory localization matters since it first sought WTO accession.[165] More recently, China has taken a different approach to these restrictive laws

159. Andrei Soldatov & Irina Borogan, *Russia's Surveillance State*, WORLD POL'Y INST. 2 (Sept. 12, 2013), http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

160. *Id.* at 3 (jumping from 265,937 intercepted phone calls and electronic messages in 2007 and 539,864 in 2012).

161. *See generally* Andrei Soldatov, *Putin Has Finally Reincarnated the KGB*, FOREIGN POL'Y 3 (Sept. 21, 2016), http://foreignpolicy.com/2016/09/21/putin-has-finally-reincarnated-the-kgb-mgb-fsb-russia/.

162. *Russian Privacy Regulator Adds Countries to List of Nations with Sufficient Privacy Protections*, HUNTON PRIVACY BLOG 1 (Aug. 16, 2017), https://www.huntonprivacyblog.com/2017/08/16/russian-privacy-regulator-adds-countries-list-nations-sufficient-privacy-protections/.

163. *Id.*

164. *See generally* Thomas Nilsen, *Staying in touch with your Russian friends via Facebook? Well, that might soon come to an end*, BARENTS OBSERVER (Sept. 27, 2017), https://thebarentsobserver.com/en/life-and-public/2017/09/staying-touch-your-russian-friends-facebook-well-might-now-come-end.

165. Raj Bhala, *Enter the Dragon: An Essay on China's WTO Accession Saga*, 15 AM. U. INT'L L. REV. 1469, 1518 (2000) (citing that China had agreed to dispense with its mandatory localization laws for CPAs).

than Russia.[166] By claiming that "without cybersecurity there is no national security," President Xi Jinping has put on an important piece of armor for protecting China's new cybersecurity law before the WTO.[167] This armor is strong because many countries are wary to attack national security protections in the WTO agreements, as they prefer to utilize them broadly themselves.[168] However, the national security provisions outlined in GATS Article XIV *bis* are restricted to three specific categories that do not overtly include protection of data, namely: provisioning the military, fissionable or fusionable materials activities, and measures taken in times of war or national emergencies.[169] Furthermore, if China recognizes the limited language of Article XIV *bis*, it will be wary of endangering other programs protected by the shroud of national security exceptions. As such, China is less than likely to raise the Article XIV *bis* defense, and even if it did, it would not hold much water. That said, China has hedged its bets by also arguing the necessity of creating privacy protections—per the same defenses discussed above in GATS Article XIV—through its cybersecurity law.[170]

Somewhat unsurprisingly, human rights activists, groups, and academics have argued that China's new law not only fails to provide necessary privacy protections for Chinese citizens, but will also actually undercut what little privacy citizens had otherwise retained under the totalitarian regime.[171] Another interesting twist in the story of China's law is the input from other nations. For example, despite detailed

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

167. *Id.*; *see also* Chiang Ling Li et al., *China's New Cybersecurity Law and Draft Data Localization Measures Expected to Burden Multinational Companies*, JONES DAY (May 2017), http://www.jonesday.com/chinas-new-cybersecurity-law-and-draft-data-localization-measures-expected-to-burden-multinational-companies-05-08-2017/.

168. *See* Matthew Kahn, *Pretextual Protectionism? The Perils of Invoking the WTO National Security Exception*, LAWFARE (July 21, 2017), https://www.lawfareblog.com/pretextual-protectionism-perils-invoking-wto-national-security-exception (explaining the dangers of raising a complaint for which a national security exception might be used).

169. GATS art. XIV *bis*.

170. Paul Triolo, Rogier Creemers & Graham Webster, *China's Ambitious Rules to Secure 'Critical Information Infrastructure'*, NEW AMERICA (Jul. 14, 2017), https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/.

171. Bethany Allen-Ebrahimian, *The 'Chilling Effect' of China's New Cybersecurity Regime*, FOREIGN POL'Y 1-2 (Jul. 10, 2015), http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security. *But see* MMLC Group, *Data Protection and Privacy Issues in China*, HG.ORG. https://www.hg.org/article.asp?id=5340 (providing a history of Chinese privacy laws and their limited effectiveness) (last visited Dec. 18, 2017).

reports generated for EU officials,[172] the EU has not challenged China's privacy reasoning as the United States has done.[173] The EU's failure to distinguish what is frankly a localization effort to collect, retain, and process Chinese citizen data only serves to undercut future arguments of necessity and conformity under GATS Article XIV,[174] as well as jeopardizes the EU's GDPR law before it even takes effect.[175] Therefore, not only would China's law stand as a legally strong target to attack on its face, but it would also imperil other data protection and privacy laws like those in the EU.

X. Governing WTO Case Law

One of the biggest frustrations for service providers is the lack of clarity of the GATS due to the small number of cases that have been brought to the WTO. Because there are few cases that have been litigated on GATS grounds, the case law for the entire agreement is very limited.[176] From that small universe of cases, there is only one case that deals with international data flows: *US–Gambling*.[177] Other cases, however, like *China–Publications and Audiovisual Products*, do provide context of how defenses are used, as well as the tests the Appellate Body has utilized to determine whether or not there was a violation of the specific provisions discussed above.[178] As analyzed below, there are various strengths and weaknesses to bringing arguments against the EU, Russia, and China for their data protection, privacy, and cybersecurity

172. *See, e.g.*, Paul de Hert & Vagelis Papakonstantinou, *The Data Protection Regime in China*, Directorate-General for Internal Policies for the European Union (Oct. 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf.

173. Mirasola, *supra* note 166.

174. Carl Schonander, *Chinese Proposed Cross-Border Data Flow Rules Contradict an Emerging International Default Norm for Cross-Border Data Flow*, Software & Info. Industry Ass'n (Apr. 19, 2017), http://www.siia.net/blog/index/Post/71824/Chinese-Proposed-Cross-Border-Data-Flow-Rules-Contradict-an-Emerging-International-Default-Norm-for-Cross-Border-Data-Flows.

175. For more details on how the Chinese Cybersecurity law operates see Courtney Bowman, Ying Li & Lijuan Hou, *A Primer on China's New Cybersecurity Law: Privacy, Cross-Border Transfer Requirements, and Data Localization*, Proskauer Privacy L. Blog (May 9, 2017), https://privacylaw.proskauer.com/2017/05/articles/international/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization/.

176. General Agreement on Trade in Services, *supra* note 94, 1869 U.N.T.S. 183.

177. *See generally* Appellate Body Report, *United States–Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (adopted Apr. 7, 2005) [hereinafter *US-Gambling*].

178. *See supra* Section II.

laws; just as there are various strengths and weaknesses for each of the countries should they pursue an Article XIV defense.

A. *U.S.–Gambling and the Article XIV Defense*

As the only real case tried before the WTO that contemplated a GATS-related question about data transfers,[179] the *U.S.–Gambling* case provides the only, albeit limited, insight into how a digital data transfers case might be analyzed by the WTO.[180] In that case, the United States argued as respondent against claims by Antigua regarding online gambling restrictions.[181] In its report, the WTO panel confirmed that electronic data transfers fell within the Mode 1 definition and subsequent commitments under GATS Article I:2.[182] Later, in the Appellate Body Report, the Appellate Body defined the legal standard for Article XVI:2, specifically subparagraphs (a) and (c), when it stated that Antigua was required to make a "prima facie case by first alleging that the United States had undertaken a market access commitment in its GATS Schedule; and secondly, by identifying with supporting evidence, how the challenged laws constitute impermissible 'limitations'" under Article XVI:2(a) or (c).[183]

In response, the United States argued an Article XIV exception.[184] Though one argument was an argument for public morals under Article XIV(a), the United States also argued under paragraph (c) that the U.S. Racketeer Influenced and Corrupt Organizations Act ("RICO") statute provided specific and "independent meaning" to protect "independent interests and values."[185] The Appellate Body responded by saying that if a Member invokes an exception under Article XIV, that member must

---

179. Nancy J. King & Kishani Kalupahana, *Choosing Between Liberalization and Regulatory Autonomy under GATS: Implications of U.S.-Gambling for Trade in Cross Border E-Services*, 40 VAND. J. TRANSNATION'L L. 1189, 1192-95 (2007).

180. *See generally US-Gambling*, *supra* note 177.

181. *Id.*

182. Panel Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 6.285, WTO Doc. WT/DS285/R (adopted Nov. 10, 2004).

183. *US–Gambling*, ¶ 143, WT/DS285/AB/R. Subsequently, the Dispute Settlement Bodies in *China-Publications and Audiovisual Products and China – Electronic Payment Services* followed the same approach. *See* Appellate Body Report, *China–Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶ 7.1354, WTO Doc. WT/DS363/AB/R (adopted Dec. 21, 2009) [hereinafter *China–Publications and Audiovisual Products*]; Panel Report, *China–Certain Measures Affecting Electronic Payment Services*, ¶ 7.511, WTO Doc. WT/DS413/R (adopted Jul. 16, 2012). *See also* Appellate Body Report, *Argentina–Measures Relating to Trade in Goods and Services*, ¶ 7.391, WTO Doc. WT/DS453/AB/R (adopted Apr. 14, 2016).

184. *US–Gambling*, *supra* note 177, ¶¶ 28-29.

185. *Id.* ¶ 29.

demonstrate "that its measure, found to be WTO-inconsistent, satisfies the requirement of the invoked defense."[186] The Appellate Body then set forth a two-tiered analysis:

> [A] panel should first determine whether the challenged measure falls within the scope of one of the paragraphs of Article XIV. This requires that the challenged measure address the particular interest specified in that paragraph and that there be a sufficient nexus between the measure and the interest protected. The required nexus - or "degree of connection" - between the measure and the interest is specified in the language of the paragraphs themselves, through the use of terms such as "relating to" and "necessary to". Where the challenged measure has been found to fall within one of the paragraphs of Article XIV, a panel should then consider whether that measure satisfies the requirements of the chapeau of Article XIV.[187]

The Appellate Body then overruled the panel's finding that the gambling prohibitions were "necessary" under Article XIV(a)[188] and because of this ruling the Appellate Body also invalidated the panel's findings with regard to Article XIV(c) because the United States could not provisionally justify its various laws used to combat gambling as "necessary within the meaning of Article XIV(c) of GATS."[189] The basis that the Appellate Body used to justify this argument, however, rested on the United States' failing to consult with Antigua, which in turn showed that the United States was unwilling to "exhaust all reasonably available alternative measures."[190]

Because this case involved a very complex fact pattern, and also rested on odd logical constructions—such as the argument against the United States exhausting all reasonably alternative measures—it is extremely difficult to draw parallels between *US–Gambling* and potential cases against data protection and localization laws. However, the case does provide a potential petitioner with an important arrow in its quiver: the WTO was willing to overrule many of the United States' most important anti-gambling rules simply because the United States failed to do everything possible to prove that the measures were

186. *Id.* ¶ 309.
187. *Id.* ¶ 292.
188. *Id.* ¶¶ 324-327.
189. *Id.* ¶¶ 335-337.
190. *Id.* ¶ 336.

"necessary" to combat the morally repugnant act of gambling. Not only was this the ruling, but as noted above, the conclusion rested on analyses that would likely be much weaker than systematic changes in rules and regulations, let alone the highly critiqued ineffectiveness of the laws used in the EU, Russia, and China.

B. *China–Publication and Audiovisual Products*

While not as expansive and on point as the *US–Gambling* case, the Appellate Body's analysis in *China–Publications and Audiovisual Products* is instructive to other potential GATS claims that would use Article XVI as their basis.[191] In *China–Publications and Audiovisual Products*, the Appellate Body confirmed that terms used in China's GATS Schedule[192] were intentionally broad enough to change over time.[193] This was a key determination because it set up an analysis for laws and schedules that would revolve around how flexible the terms and definitions would be applied to changing technology. Furthermore, the Appellate Body also found that under Article XVI, a Member agrees to provide a minimum standard of treatment, and is thus free to maintain a market access regime less restrictive than set out in its schedule.[194] This means that should the United States bring a case against the EU, Russia, or China, it could argue that each of those countries had violated its GATS Article XVI obligations because each of the schedules of commitments for those countries requires a minimum standard of treatment for incoming and outgoing data flows that is not being upheld due to the burdensome laws and regulations.

XI. Interpreting GATS Through New Trade Agreements

According to one author, "aspects of the GATS should be considered a 'living agreement,'" meaning that commitments made under the agreement are considered constantly evolving and changing.[195] Because protecting citizen privacy is not necessarily connected with localization requirements or data transfer restrictions, it may prove helpful for the United States to also look to other trade agreements for context. It should be noted, however, that the WTO Appellate Body has been hesitant to apply standards in other trade agreements in its analysis outside

191. *See generally* Appellate Body Report, *China–Publications and Audiovisual Products*, WTO Doc. WT/DS363/AB/R (adopted Dec. 21, 2009).

192. "Sound recording" and "distribution."

193. *China–Publications and Audiovisual Products*, *supra* note 183, ¶¶ 295-96.

194. *Id.* ¶ 7.1353.

195. Crosby, *supra* note 22, at 4.

of the Vienna Convention on the Law of Treaties.[196] Despite this resistance by the WTO Appellate Body, other treaties may include language from many of the WTO member states that better reflects their demands regarding data transfers.

A. *Negotiating Objectives and Current Agreements for the United States*

Because it is, by far, the largest services exporter,[197] the United States would benefit more than any other WTO member by winning a case against the EU, China, or Russia.[198] Additionally, the United States does not have a sophisticated privacy regime, but rather protects against disruptions of privacy through contract.[199] As such, the United States would also not need to worry about a ruling severely limiting excepted laws vis-à-vis GATS Article XIV(c)(ii). As such, an analysis of the provisions the United States has included in its most recently negotiated trade agreements provided in the following section.

1. U.S.-Korea Free Trade Agreement ("KORUS")

KORUS is widely considered among trade authorities in the United States as the most updated and implemented legal text on the regulation of data transfers.[200] The financial services chapter provides that "[e]ach Party shall allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the institution's ordinary course of business."[201] Although the United

196. Chang-fa Lo, *The Difference Between Treaty Interpretation and Treaty Application and the Possibility to Account for Non-WTO Treaties During WTO Treaty Interpretation*, 22 IND. INT'L COMP. L. REV. 1, 2 (2012), http://mckinneylaw.iu.edu/iiclr/pdf/vol22p1.pdf (noting that the VCLT is referenced mainly because many of the referenced provisions are simply seen as a codification of customary international law).

197. *Service Exports in Current Prices*, KNOEMA: WORLD DATA ATLAS (citing *Service Exports (BoP, Current US$)*, WORLD BANK, https://data.worldbank.org/indicator/BX.GSR.NFSV.CD?end=2016&start=2016&view=map (last visited Dec. 18, 2017)), https://knoema.com/atlas/ranks/Service-exports (last visited Dec. 18, 2017).

198. Another reason for this is because the United States would not be concerned about the need to protect citizen privacy vis-à-vis GATS art. XIV(c)(ii); as such, it would have the least to lose compared to other major services exporters.

199. *See, e.g.*, *Enforcing Privacy Promises*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Dec. 18, 2017).

200. Diane A. MacDonald & Christine M. Streatfeild, *Personal Data Privacy and the WTO*, HOUS. J. INT'L L. 625, 631-32 (2014), http://www.hjil.org/articles/hjil-36-3-macdonald-streatfeild.pdf.

201. Free Trade Agreement, S. Kor.-U.S., Annex 13-B § B, Mar. 15, 2012 [hereinafter KORUS], https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file35_12712.pdf.

States already allowed this at the time, South Korea had a restriction that required localization of financial data and prevented that data from being transferred outside the country for processing.[202] While the text itself is meaningful, it should be noted that the provision continues to cause some consternation for U.S. companies who argue that South Korea is not living up to its commitments by still requiring individual consent be secured and recorded by financial services firms before transferring consumer data.[203] Due to the failure of the TPP rounds, KORUS is still widely considered the gold standard when it comes to data transfer language.[204]

2. TPP and NAFTA 2.0

The TPP was intended to work as the upgraded "gold standard" agreement,[205] beyond KORUS.[206] Despite being scrapped in the first

202. MacDonald & Streatfeild, *supra* note 200, at 630 (citing *U.S., EU Engaged with Korea on Implementation of Data-Flow Obligation*, INSIDE U.S. TRADE, (June 7, 2013)); *see also* Chander & Le, *supra* note 118 (providing more detail on South Korean laws requiring localization).

203. U.S. officials state that Korea has put in place the necessary regulations and guidelines for implementing the data transfer provision. However, how these rules will work in practice remains a question. *Official: U.S. Hopes to Consult Further with Korea on TPP Within Weeks*, INSIDE U.S. TRADE (Mar. 20, 2014), http://insidetrade.com/201403172464544/WTO-Daily-News/ Daily-News/official-us-hopes-to-consult-further-with-korea-on-tpp-within-weeks/menuid-948.html.

204. *KORUS FTA Facts: New Opportunities for Financial Services*, OFF. OF THE U.S. TRADE REPRESENTATIVE (Oct. 2008), https://ustr.gov/archive/assets/Document_Library/Fact_Sheets/2008/asset_upload_file972_15191.pdf. It should also be noted that While there is not space to adequately treat it, South Korea also signed a trade agreement with the EU. MacDonald & Streatfeild, *supra* note 200, at n. 23. Also, just a few months earlier, Korea had entered into an identical commitment in the European Union-Korea Free Trade Agreement. Memorandum from the European Commission on the Ten Key Benefits for the EU from the EU-Korea Free Trade Agreement (Sept. 17, 2010), http://europa.eu/rapid/press-release_MEMO-10-423_en.htm (noting that pursuant to that agreement, Korea pledged to allow these transfers by July 1, 2013).

205. *See, e.g.*, Glenn Kessler, *Fact Check: Clinton Did Call TPP 'the Gold Standard,'* WASHINGTON POST (Sept. 26, 2016), https://www.washingtonpost.com/politics/2016/live-updates/general-election/real-time-fact-checking-and-analysis-of-the-first-presidential-debate/fact-check-clinton-dod-call-tpp-the-gold-standard/?utm_term=.aa6ba3408f6c (citing a speech then Secretary of State Hillary Clinton gave in Australia, where she noted "This TPP sets the gold standard in trade agreements to open free, transparent, fair trade . . . .")

206. Neha Mishra, *The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?*, 20 J. INT'L ECON. L. 31 (2017), https://advance.lexis.com/api/permalink/21caa43f-5874-4445-b9c4-e991e5e773c6/?context=1000516. *But see* Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-border Data Transfer*, 19 YALE J. L. & TECH. 182, 236 (2017), https://advance.lexis.com/api/permalink/f5332fbc-487c-4b94-8266-d048b11b49b0/?context=1000516.

few days of its administration,[207] the Trump administration has adopted many of the same arguments as the Obama administration on cross-border data flows and localization requirements.[208] These same arguments are also being made by major trade associations who urge that an update to the United States' trading relationship language with Canada and Mexico holds "significant potential for the internet economy."[209] Furthermore, while discarded, the TPP also included Mexico and Canada, both of whom had agreed in principle to language that would prohibit localization requirements.[210]

Importantly, the TPP also included language on protecting personally identifiable information, in Article 14.8, and discussed cross-border data transfers and localization in Articles 14.11 and 14.13.[211] However, while these are the negotiating positions of the United States, it does not mean that the United States believes that all other GATS members who have included covered services in their commitments would share the same views on open transfers. However, the United States can counter these assertions by explaining that data transfers language has only recently been negotiated in trade agreements just to clarify the original intention of the GATS and ensure data transfers are allowed across borders regardless of exceptions listed in each countries' GATS scheduled commitments. It will be critical for the United States to take the right tone here and more research should be done with respect to South

207. Peter Baker, *Trump Abandons Trans-Pacific Partnership, Obama's Signature Trade Deal*, N.Y. TIMES (Jan. 23, 2017), https://www.nytimes.com/2017/01/23/us/politics/tpp-trump-trade-nafta.html?_r=0.

208. *Compare The Trans-Pacific Partnership*, USTR, https://ustr.gov/sites/default/files/TPP-Promoting-Digital-Trade-Fact-Sheet.pdf (last visited Dec. 18, 2017), *with Summary Objectives for the NAFTA Renegotiation*, USTR 8-9 (Jul. 17, 2017), https://ustr.gov/sites/default/files/files/Press/Releases/NAFTAObjectives.pdf.

209. *See, e.g.*, *Modernizing NAFTA for Today's Economy*, INTERNET ASSOCIATION, https://internetassociation.org/wp-content/uploads/2017/06/Modernizing-NAFTA-White-Paper.pdf (last visited Dec. 18, 2017).

210. Vicki Needham, *Obama Administration Strikes Deal on TPP Data Storage*, HILL (May 25, 2016), http://thehill.com/policy/finance/trade/281294-obama-administration-strikes-deal-on-data-storage-concerns-in-tpp. *See also A New Approach to Data Localization and Financial Services*, INSIDE TRADE, https://insidetrade.com/sites/insidetrade.com/files/documents/may2016/wto2016_1297a.pdf (citing the Obama Administration's commitment to seeking similar outcomes in all other trade agreements) (last visited Dec. 17, 2017); Rachel F. Fefer, *TPP Financial Services Data Flows*, FEDERATION OF AMERICAN SCIENTISTS (June 3, 2016), https://fas.org/sgp/crs/row/IN10498.pdf.

211. For a discussion of these provisions see William J. Drake, *Data Localization and Barriers to Transborder Data Flows* 15-16 (World Econ. F., Background Paper, 2016), http://www3.weforum.org/docs/Background_Paper_Forum_workshop%2009.2016.pdf.

Korea's scheduled commitments as compared to the scheduled commitments made by Russia, China, and the EU.

B. *Building in a New Defense for Privacy: European Union Negotiations and Agreements*

The EU has taken a different position. The EU has recently taken to explicitly stating the need to retain laws and regulations that promote privacy protections and limit unrestricted data transfers out of the EU. Two recent agreements, one passed and one on hold, help to explain both the goals of the EU, as well as what they are willing to accept in a final agreement—albeit with a very like-minded WTO member.

1. The EU-Canada Comprehensive Economic and Trade Agreement ("CETA")

One of the EU's most recent trade agreements is CETA.[212] While Canada's laws are considered to provide adequate protections for EU citizens, the bilateral agreement specifically includes language in its e-commerce section that "calls for respect of privacy laws, both for the private and public sectors, as well as privacy as a fundamental right."[213] The EU has repeatedly asserted that free trade "doesn't mean lowering or changing EU standards that protect people's health and safety, social rights, [or] their rights as consumers," and the EC has asserted that these same principles are protected in CETA.[214]

Specifically, in Article 16.4, CETA requires that both parties should "adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce."[215] Importantly, the text continues by vaguely referencing "international standards of data protection" expressed by "relevant international organisations of which both Parties are a member."[216] While not citing the WTO specifically, there are few other groups that regulate trade in services of which both countries are members.

---

212. *CETA Explained*, EUROPEAN COMMISSION, http://ec.europa.eu/trade/policy/in-focus/ceta/ceta-explained/ (last visited Dec. 18, 2017).

213. Patrick Zingerle, *Trade Agreements and Data Flows: Safeguarding the EU Data Protection Standards*, EU-LOGOS, https://europe-liberte-securite-justice.org/2015/07/30/trade-agreements-and-data-flows-safeguarding-the-eu-data-protection-standards/ (last visited Dec. 18, 2017).

214. *CETA Explained*, *supra* note 212.

215. *CETA Chapter by Chapter*, EUROPEAN COMMISSION: DIRECTORATE-GENERAL FOR TRADE, http://ec.europa.eu/trade/policy/in-focus/ceta/ceta-chapter-by-chapter/ (last visited Dec. 18, 2017).

216. *Id.*

Even if the groups being referenced do not include the WTO, the meeting of the minds on this issue would impair any argument that privacy laws that protect consumers are not intended in GATS Article XIV. Thus, the United States will need to be very specific about the necessity and consistency of such laws.

2. The Transatlantic Trade and Investment Partnership ("TTIP")

Due to the fragility of data transfers between the EU and the United States at the time, the EU, breaking with tradition, publicly disclosed its negotiating position on privacy for TTIP.[217] The EU's position closely imitates GATS Art. XIV(c)(ii).[218] This is important because the EU easily could have sought more protections and assurances from the United States because of the failure of the United States-EU Safe Harbor program.[219] Because the TTIP is currently on hold, the inclusion of virtually identical language to GATS Art. XIV(c)(ii) also indicates the EU's strong reliance on the text as agreed to in GATS. One report, argues, however, that creating a finalized TTIP agreement that balances privacy and data flows would help cement the EU's case in what would otherwise be a very difficult WTO challenge for the EU.[220] This area is highly contentious, however, with EU Parliament members publicly calling for an exclusion of information transfers in TTIP.[221] Due to these difficulties, as well as other political issues within the EU,[222] it is hard to see an agreement concluding any time soon between the EU and the United States that will cover such transfers and explain how the United States and EU's transfer positions might mesh. This rift may actually prove helpful to the United States, as it can argue that the new EU-U.S. Privacy Shield program[223] exceeds the baseline established in GATS Article XIV.

---

217. Greenleaf, *supra* note 128.

218. *Id.*

219. *Id.*; *see also* Pham, *Dark Clouds: Privacy Law as a Barrier to Trade in Cloud Computing* 27 (CITBA, Paper No. 9, 2015), http://www.citba.org/documents/2015-Pham.pdf.

220. *See generally* Erica Wiking Haeger & Carolina Dackoe, *Data Flows: Allowing free trade agreements to strengthen the GDPR*, MANNHEIMER SWARTLING (Oct. 19, 2016) http://www.mannheimerswartling.se/globalassets/publikationer/data-flows.pdf.

221. Zingerle, *supra* note 213.

222. For instance, Wallonia's rejection of CETA and Brexit are two major examples of these issues.

223. *Privacy Shield Overview*, U.S. DEP'T OF COMM., https://www.privacyshield.gov/Program-Overview (last visited Dec. 17, 2017).

C. *Adapting Newcomers to Liberalizing Trade Deals: Russia and China*

While the United States and the EU have a long history of striking trade deals seeking reduced barriers to entry, Russia and China find themselves in a much different position, only more recently seeking out free trade agreements with other trading partners. As comparative newcomers to trade agreements, both Russia and China are still developing their own approaches to data transfers, privacy, and localization language. As indicated in the following section, the current agreements say little on the subject, though there seems to be a strong impetus for moving in a direction with fewer barriers to digital transfers.

1. India-Russia/EAEU Trade Agreement

Other than its long-time trading partnerships within the EAEU, Russia had remained a relatively insular trader until its WTO accession in 2012.[224] Since its accession, Russia's status within the WTO has been controversial,[225] but that controversy has not impeded Russia and India from seeking a trade agreement with each other.[226] While still negotiating the text, India's reluctance to include an e-commerce chapter in the agreement should raise some flags.[227] India's telecommunications and technology sectors might be at odds over localization,[228] but Russia's focus has mainly been on including provisions that cover mutual recognition of electronic signatures and electronic documents, not on ceding ground on localization measures.[229] Russia is difficult to read when it comes to having a position on electronic transfers, telecommunications, and privacy protections. What is known is that Russia is home to one of the strictest localization regimes of all WTO countries, and its

224. *Russia – Trade Agreements*, U.S. DEP'T OF COM., https://www.export.gov/article?id=Russia-Trade-Agreements (last visited Dec. 17, 2017).

225. Hans von der Burchard, *EU bid to appease Russia over Ukraine deal collapses*, POLITICO (Dec. 21, 2015), https://www.politico.eu/article/ukraine-russia-fta-tade-eu/.

226. Dipanjan Roy Chaudhury, *India, Russia plan Free Trade Agreement in Eurasian region*, ECON. TIMES, https://economictimes.indiatimes.com/news/economy/foreign-trade/india-russia-plan-free-trade-agreement-in-eurasian-region/articleshow/58885682.cms (updated May 29, 2017).

227. Asit Ranjan Mishra, *India not keen to put e-commerce under FTA with Russia-led group*, LIVE MINT (May 29, 2017), http://www.livemint.com/Politics/OUXyKIwZHpnoJPhj6mfuyK/India-not-keen-to-put-ecommerce-under-FTA-with-Russialed-g.html.

228. *Id.*

229. *Id.*

operating trade agreements,[230] even with the EU, share limited details on how other countries are to cope with Russian rules and regulations.

2. The China-Australia Free Trade Agreement ("ChAFTA")

In December 2015, the ChAFTA came into force.[231] Chapter 12 of that agreement specifically addresses electronic commerce and includes a section, Article 12.5, which closely parallels GATS Article VI, by stating that each party commits to "minimise the regulatory burden on electronic commerce; and ensure that regulatory frameworks support industry-led development of electronic commerce."[232] Article 12.8 specifically addresses consumer data privacy and requires that both countries "take such measures . . . appropriate and necessary to protect the personal information of users of electronic commerce."[233] The agreement then references adherence to the rules of international organizations, and specifically cites to the WTO for authority in Article 12.1.[234]

Furthermore, while localization is not addressed in the agreement specifically,[235] China has overtly taken an increasingly liberal approach to trade with Australia; in fact, in early 2017, China began expanding its e-commerce trade with Australia by reducing some of the regulations it has on vitamins and baby food products.[236] The vice minister for foreign affairs, Zheng Zeguang, noted at the time that China was "committed to a greater level playing field and promoting the sound development of retail imports in cross-border e-commerce."[237] Some have argued this

230. *See Russia*, EUROPEAN COMMISSION: DIRECTORATE-GENERAL FOR TRADE, http://ec.europa.eu/trade/policy/countries-and-regions/countries/russia/ (providing a history of EU trade relations with Russia) (last visited Dec. 18, 2017).

231. *China-Australia Free Trade Agreement*, AUSTL. DEP'T OF FOREIGN AFFAIRS AND TRADE, http://dfat.gov.au/trade/agreements/chafta/pages/australia-china-fta.aspx (last visited Dec. 18, 2017).

232. Free Trade Agreement, Austl.-China, art. 12.5(2)(a)-(b), Dec. 20, 2015, Austl. Dep't of Foreign Affairs and Trade, http://dfat.gov.au/trade/agreements/chafta/official-documents/Documents/chafta-chapter-12-electronic-commerce.pdf.

233. *Id.*

234. *Id.*

235. Neither are there any provisions, notably, included in the financial services side letters. *See* Andrew Robb, *ChAFTA Side Letter on Financial Services* (June 17, 2015), http://dfat.gov.au/trade/agreements/in-force/chafta/official-documents/Documents/chafta-side-letter-on-financial-services.pdf.

236. Kirsty Neeham, *China wants to expand e-commerce*, SYDNEY MORNING HERALD (Mar. 21, 2017), http://www.smh.com.au/business/retail/china-wants-to-expand-ecommerce-trade-with-australia-20170321-gv2xed.html.

237. *Id.*

change in policy has arisen due to China's Alibaba group becoming heavily invested in liberalization of ecommerce.[238]

3. The Regional Comprehensive Economic Partnership ("RCEP")

The RCEP is a free trade agreement aimed at broadening regional ties, integration, and liberalizing trade and investment between the 10 ASEAN economies, as well as Australia, China, India, Japan, Korea, and New Zealand.[239] With around $17 trillion of trade accounted for among the nations, the agreement is the largest mega-regional agreement under negotiation.[240] As part of those negotiations, a working group on e-commerce ("WGEC") has been established, and leaked chapters indicate that there is at least some consideration of anti-localization measures in the e-commerce chapter.[241] However, because this agreement is far from concluded, it acts merely as speculation on China's position, but when taken in tandem with China's new approach to trade with Australia as outlined above, it seems clear that China may be willing to loosen some of its regulations for its trading partners and has not cited privacy or security concerns. This change in approach collides with China's cybersecurity policies and would considerably undercut arguments for an Article XIV exception for those laws.

XII. Conclusion

Because the EU, China, and Russia have all made very specific commitments in their GATS schedules, have floundered in precise implementation of each of their laws, and will likely have difficulty arguing that each of the laws the countries have implemented are both necessary and consistent as required by the GATS Article XIV exception, the United States would likely find at least some success if it were to bring a case against the laws in each of these countries. However, as noted above, the limited case law makes it extremely difficult to predict how the Appellate Body will evaluate specific claims against the EU, China, or Russia. Furthermore, the fact that localization requirements are just now being addressed through trade agreements makes it more difficult

238. Goenuel Serbest, *China moves to strengthen e-commerce ties with Australia*, Trade Victoria (Mar. 24, 2017), http://trade.vic.gov.au/news/2017/feb2/china-moves-to-strengthen-e-commerce-ties-with-australia.

239. Jyoti Panday, *RCEP Discussions on Ecommerce: Gathering Steam in Hyderabad*, Elec. Frontier Found. (Jul. 24, 2017), https://www.eff.org/deeplinks/2017/07/rcep-discussions-ecommerce-gathering-steam-hyderabad.

240. *Id.*

241. *Id.*

for the United States to argue that these barriers were contemplated or at least envisioned when the GATS was signed by each of the member states.

At the same time, the limited case law that currently exists would make an Article XIV defense very difficult for the EU, Russia, or China to assert. Therefore, the United States would likely find success in reducing or eliminating the localization and privacy trade barriers to digital transfers in the EU, China, and Russia. The extent of success, however, will likely vary from member to member.

A. *China*

Out of the three countries, China's cybersecurity laws are likely to be viewed by a WTO panel as most starkly in violation of the GATS. China's schedule of commitments was made during the dotcom boom, and while they provide some limited carve-outs, the remaining commitments are likely to be found by any WTO panel to include a broad swath of digital transfers and other digital services. To make matters more difficult, China will have the most difficult time of the three WTO members justifying its cybersecurity laws under an Article XIV privacy defense. Furthermore, an Article XIV defense would likely be considered not only unlikely to succeed but also very unpalatable to China because it could endanger other GATT and GATS violating laws backed by national security defenses. As such, a complaint brought by the United States would almost certainly find success before a WTO panel so long as China continues on its present course. Should China wish to avoid losing such a complaint, it would be helpful for them to concretely ground their cybersecurity laws on privacy grounds, set up a data protection authority, and possibly revise their scheduled GATS commitments given China's long-standing restrictions against digital transfers.

B. *Russia*

Russia's localization laws are perhaps most precarious because they are widely recognized as two-faced. Despite efforts from Roskomnadzor, Russia's data protection authority, to assert the privacy purposes in the localization laws, the broad authority granted to the FSB to conduct warrantless searches on the now-localized servers calls into question not only whether the laws are actually intended to provide privacy, but also if the laws are created in a way that would be considered compliant with a GATS Article XIV exception. Certainly, the United States would very likely argue successfully to a WTO panel that Russia's laws provide

limited, if any, real privacy to citizens, and even if they did, the privacy that might be provided is not done in a necessary and consistent way. Furthermore, Russia's refusal to acknowledge the EU's long-standing recognition as a premiere privacy-protecting WTO member will further hamstring an Article XIV defense. Finally, Russia's late accession to the WTO provides any WTO panel with one of the timeliest commitment schedules available—a commitment schedule that broadly commits to open-transfers of telecommunications and digital information. Given Russia's already rocky relationship with the United States and many other WTO members, a revision of those commitments would likely produce significant backlash. As such, Russia should look to amend their localization laws to purely provide privacy protections. If the laws continue as presently constructed, it is difficult to imagine any way Russia can assert justification for the laws on their face before a WTO panel.

C. *European Union*

The EU provides the most complex and arduous complaint for the United States, but it also provides the most rewarding. A significant portion of the $400 billion in digital trade each year flows into or out of either the United States and the EU, and with the broad territorial reach of the EU's new GDPR law, the EU is seeking to create a new baseline in privacy protections and digital transfer restrictions that could forever change the corresponding interpretation of GATS commitments with regard to data transfers. While the EU has long been considered the vanguard of privacy protections for consumers, comments made by EU officials themselves, as well as many other academics, professionals, and other researchers indicate that the GDPR may not fit under the necessary and consistent requirements required for a GATS Article XIV defense, per the Appellate Body's ruling in *US-Gambling*. Furthermore, the overlapping laws and restrictions of the EU generally and the individual EU member states will make the necessary and consistent arguments very difficult for drafters of the EU's response to a U.S. complaint.

The EU has one big advantage over Russia and China, though: it shares an increased likelihood of winning—which would be devastating for the United States—and even if it did lose, it would likely be because of the GDPR and other individual localization requirements for each of the individual EU member states. The EU can then agree to alter its laws, creating a virtually identical regime that would need to be verified and reviewed by the WTO again. This long cycle of complaint, response, panel report, and Appellate Body review, followed by

amendment, review, and judgment of further laws and regulations would likely take years. During those years, the damage might very likely already be done. If, however, the United States were to get judgments or settlements with Russia and China, it might provide meaningful traction and impetus that would almost certainly both speed up the process and give the United States an upper hand in negotiations. As such, the EU should work to keep the United States from bringing any case of data flows before the WTO, as well as work with countries that improperly cite privacy protections as the purpose for their localization and cybersecurity laws and regulations. No matter how the United States or the EU act in the future, however, the actions or inactions that carry the day are likely to set the regulatory tone for the majority of global trade over the WTO's next twenty-five years.