Regulation of Data Localization and How the Legal Profession Can Play a Role

KAITLYN TSAI*

INTRODUCTION

In the last few decades, the significant growth of the Internet and other digital technologies has given rise to numerous industries that rely heavily on the ability to collect, aggregate, process, and transfer information across borders.[1] Concurrently, traditional industries, such as manufacturing and agriculture, have grown more dependent on access to data to monitor supply chains, support products in the field in real time, and manage workforces.[2] Cross-border data flows, accordingly, have become crucial in enabling international trade, which can lead to increased innovation, productivity, and economic growth.[3] In the coming years, as the world continues to increase its dependence on technology, cross-border data flows are expected to grow at a rate faster than the overall rate of global trade.[4]

Despite the obvious importance of cross-border data flows, recently countries scattered throughout the world have begun enacting varying degrees of data restrictive regulation to limit the flow of data outside their borders.[5] Data localization measures are one such way of restricting data flows. Data localization measures are any legal limitation on the ability of data to move globally and can encompass a wide range of requirements including the localization of data servers and providers, local content policies, and consent mandates for data transfers, for

---

* J.D., Georgetown University Law Center (expected May 2022); B.S., University of California, Berkeley (2015).

1. Susannah Hodson, *Applying WTO and FTA Disciplines to Data Localization Measures*, 18 WORLD TRADE REV. 579, 579–80 (2018).

2. *See* NIGEL CORY, INFO. TECHNOLOGY & INNOVATION FOUND., CROSS-BORDER DATA FLOWS: WHERE ARE THE BARRIERS, AND WHAT DO THEY COST, INFORMATION TECHNOLOGY & INNOVATION FOUND. 1, 1. (2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost [https://perma.cc/KH7T-XFDB].

3. *See* MICHAEL MANDEL, PROGRESSIVE POL'Y INST., DATA, TRADE AND GROWTH 2 (2014) (quoting Joshua Meltzer, BROOKINGS INST., THE INTERNET, CROSS-BORDER DATA FLOWS, AND INTERNATIONAL TRADE, (Feb. 2013)), https://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf [https://perma.cc/7WC5-27H4].

4. *See* CORY, *supra* note 2.

5. *See generally* JOSHUA P. MELTZER & PETER LOVELOCK, GLOBAL ECON. AND DEV. AT BROOKINGS, REGULATING FOR A DIGITAL ECONOMY: UNDERSTANDING THE IMPORTANCE OF CROSS-BORDER DATA FLOWS IN ASIA, (Mar. 2018), https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf [https://perma.cc/7M3F-3K3U].

example.[6] In the last decade, there has been a proliferation of data localization measures as a growing number of countries impose rules forcing data to be kept within their own borders.[7]

Governments cite a variety of reasons for utilizing data localization measures, including protecting national security interests, protecting privacy of their citizenry, ensuring greater economic opportunities for domestic digital players, and maintaining public order.[8] Yet, it remains unclear just how effective these measures are at helping governments achieve their public policy goals. [9] What is clear, however, is that data localization stands at odds with the modern-day digital economy that depends on the ability of data to move "expeditiously and efficiently" across countries—or, in other words, the free flow of data.[10] The movement of many countries towards more stringent data localization measures risks potentially devastating consequences. One major concern is that data localization may impede trade in services and hinder continual economic integration. Furthermore, data localization can raise the cost of doing business, slow down innovation, and could eventually balkanize the Internet.[11]

At the moment, there are few specific rules targeting data flows on the international level to effectively safeguard against overreaching data localization measures. Some experts have suggested that the WTO is the proper institution to provide an adequate framework to address cross-border data flow issues.[12] This Note argues that the WTO is inadequate as a venue and as a source of norms to prevent future data localization measures. Rather, given the complexity and the competing interests that drive the implementation of data localization measures, a diverse set of novel solutions created with the coordination of various stakeholders, including lawyers, would more effectively address the problem. These solutions include creating a data flow framework, establishing an independent dispute settlement body to assess the legality of data restrictive measures, involving lawyers to help companies navigate data localization measures, and utilizing the broader legal community to help lawyers better navigate changes in data flow policy.

---

6. *See* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015).

7. Joshua P. Meltzer, *Data and the Transformation of International Trade*, BROOKINGS INST. (Mar. 6, 2020), https://www.brookings.edu/blog/up-front/2020/03/06/data-and-the-transformation-of-international-trade/ [https://perma.cc/C7PL-QW3W]; MARTINA F. FERRACANE, RESTRICTIONS ON CROSS-BORDER DATA FLOWS: A TAXONOMY 2 (2017); Benjamin Wong, *Data Localization and ASEAN Economic Community*, 10 ASIAN J. INT'L L. 158, 159 (2020).

8. *Id.*

9. *See* Adrian Shahbaz, Allie Funk, Andrea Hackl, *User Privacy or Cyber Sovereignty? Assessing the Human Rights Implications of Data Localization*, FREEDOM HOUSE (July 2020), https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty [https://perma.cc/6FZC-FU8D].

10. Andrew D. Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How the WTO Law Can Contribute*, 22 J. INT'L ECON L. 389, 390 (2019).

11. *See* Wong, *supra* note 7, at 159; Shahbaz et al., *supra* note 9.

12. *See e.g.,* Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Be In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer,* 19 YALE L.J. & TECH. 182, 186 (2017).

First, this Note will identify the common arguments governments cite when they choose to localize data. In Part II, the Note will explore the costs of data localization and concludes that the costs likely outweigh the purported benefits data localization confers. Part III will evaluate the effectiveness of the WTO in helping prevent excessive data localization measures. In Part IV, this Note will present alternative solutions to the multilateral framework to help regulate data localization and discusses the role that the legal profession can play in both the international and domestic front in helping develop these solutions.

I. CONCERNS DRIVING IMPLEMENTATION OF DATA LOCALIZATION MEASURES

Countries have implemented a range of data localization measures for a variety of policy objectives. To determine the best solutions to address challenges that arise from data localization, a good starting point is to assess the policy reasons behind countries' implementation of data localization measures

A. NATIONAL SECURITY

National security is a common rationale that governments use to justify implementing data localization measures.[13] As data flows become increasingly important for the global economy, governments have also begun to fear that the free flow of data may allow foreign adversarial governments to access and collect sensitive information, which could ultimately pose serious national security threats.[14] This scenario is especially pertinent when the governments of foreign adversaries can easily gain access, without having to provide any justification, to any information that flows through their territories.[15] To safeguard against these potential national security threats, countries sometimes choose to localize their data in hopes that sensitive information can stay protected within their borders.[16] For example, facing the overt threat of rival North Korea, South Korea bars companies from using mapping data not stored within South Korean territory.[17]

---

13. *See* Lothar Determann, *How Data Residency Laws Can Harm Privacy, Commerce, and Innovation—and Do Little for National Security,* WORLD ECONOMIC FORUM (June 9, 2020), https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/ [https://perma.cc/8JAH-Y82R].

14. *See* INST. INT'L FINANCE, DATA FLOWS ACROSS BORDERS: OVERCOMING DATA LOCALIZATION REQUIREMENTS 4–5 (2019), https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf [https://perma.cc/KD9N-KKGN].

15. *See id.*

16. *See* Wong, *supra* note 7, at 162.

17. William Alan Reinsch & Andrew Lepczyk, A Data Localization Free-for-All?, Ctr. for Strategic & Int'l Studies (Mar. 9, 2018), https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all [https://perma.cc/NQ3N-3YF4].

Shockingly,[18] the United States, which has historically been a strong proponent of open data flows,[19] has also taken actions resembling data localization measures seen in other parts of the world. On August 14, 2020, President Donald Trump issued a Committee on Foreign Investment in the United States Order ("CFIUS Order") demanding that ByteDance, the parent company of the social media application, TikTok, divest all of its rights and interests in any assets or property used to enable or support the operation of TikTok in the United States, and "any data obtained or derived from TikTok or Music.ly application users in the United States" within ninety days.[20] In essence, the U.S. government presented ByteDance with two choices: to sell some or all of its interest in TikTok to U.S. entities or to have TikTok banned from the U.S.[21] President Trump reasoned that he was doubling down because TikTok's affiliation with the Chinese Communist Party ("CCP") presented threats to "national security, foreign policy, and the economy of the United States."[22] In the end, Oracle and Walmart agreed to take a minority stake in TikTok and Oracle won the right to sell cloud services to TikTok, meeting the U.S. government's demand that TikTok user data be stored in the United States.[23] The United States' move toward more data restrictive policies (including data localization) is an alarming signal because, as the world leader, it may cause a protectionist response and encourage other countries to follow suit.

---

18. The United States has historically been a strong supporter of the free flow of data. In 1997, for example, President Bill Clinton's administration declared that "the U.S. government supports the broadest possible free flow of information across international borders" and presented the first set of global principles regarding the governance of cross-border data flows, known as the Framework for Global Electronic Commerce. The U.S. further pushed for the free flow of data when it became the leading force behind the WTO's moratorium on taxes on cross-border data flows. Both the Bush and Obama administration subsequently continued to push for the free flow of data. For example, the Obama administration made digital trade issues a major focus and was determined to respond to policies that influential US companies deemed protectionists. The administration turned to bilateral and regional trade agreements to regulate such practices and urged countries to "endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders." The Trump administration, on the other hand, took a radically different approach to digital trade than its predecessors. In contrast to previous administrations, the Trump administration has deviate from the U.S.' historical advocacy for the free flow of information across borders, such as rejecting the net neutrality principle and taking measures to localize data, as seen with the TikTok and WeChat Executive Orders. Susan A. Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms, and Its Implications for the WTO*, 21 J. INT'L ECON. L. 245, 253–58 (2018).

19. *See e.g.*, RACHEL F. FEFER, CONG. RSCH. SERV., DATA FLOWS, ONLINE PRIVACY, AND TRADE POLICY 2 (2019).

20. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020); Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (Aug. 6, 2020).

21. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020); Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (Aug. 6, 2020).

22. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020); Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (Aug. 6, 2020).

23. Jordan Novet, Spencer Kimball & Alex Sherman, *Trump Agrees to TikTok Deal with Oracle and Walmart, Allowing App's U.S. Operations to Continue*, CNBC (Sep. 19, 2020), https://www.cnbc.com/2020/09/19/trump-says-he-has-approved-tiktok-oracle-deal-in-concept.html [https://perma.cc/4GZK-SEEK].

Data localization measures are now increasingly being used as a means to address national security concerns.[24] Whether these measures are actually effective in mitigating national security threats is subject to debate. Chander and Lê argue that the data localization measures are ineffective because foreign surveillance continues to occur even after data is stored locally.[25] Technologies such as malware allow for adversarial governments to infiltrate networks and collect data on a large scale without ever requiring agents to set foot on the ground of the target country.[26] Even if the target country keeps information locally stored, malware can be used to hack systems remotely and enable the data to be accessed from any part of the world. Other experts argue that localization requirements may actually make it easier for foreign adversaries to conduct surveillance, because data stored in one place or a few concentrated places eases the logistical burdens for foreign adversaries collecting information.[27] Additionally, data localization may "compel[] companies to use [local data storage providers] rather than global ones."[28] Local storage providers often have fewer resources and therefore are more likely to have weaker security infrastructure.[29] Therefore, data stored on local servers may ultimately be at higher risk of breach.[30]

B. PRIVACY

Some countries enact data localization measures to try to protect the privacy of their citizens and confidential information possessed by their businesses.[31] Although data localization requirements designed to protect privacy have existed for as early as 2005,[32] the 2013 Edward Snowden affair, which revealed shocking evidence of invasive U.S. surveillance targeting American and foreign citizens, increased governmental pressures to protect data and pushed many countries to introduce data localization measures.[33]

---

24. *See* Chander & Le, *supra* note 6 at 713–14.
25. *Id*. at 715–18.
26. *Id*. at 719.
27. *Id*. at 717.
28. *Id*. 716.
29. *Id*. at 716–17.
30. *Id*. at 717.
31. *See* Mitchell & Hepburn, *supra* note 12, at 192.
32. Neha Mishra, *Data Localization Laws in a Digital World: Data Protection or Data Protectionism?,* THE PUBLIC SPHERE 136, 139 (2016).
33. In 2013, Edward Snowden, a former contractor for the CIA, leaked to the media details of extensive Internet and phone surveillance by American intelligence. Snowden revealed that the National Security Agency (NSA) tapped directly into the servers of nine internet firms, including Facebook, Google, Microsoft, and Yahoo, to track online communication in a surveillance program called Prism. *Edward Snowden: Leaks that Exposed US Spy Programme,* BBC (Jan 17, 2014), https://www.bbc.com/news/world-us-canada-23123964 [https://perma.cc/WW7M-XSAT]; Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders,* 2 THE LAWFARE RESEARCH PAPER SERIES 1, 2–3 (2014).

It is important to note that data localization measures used to protect privacy do not all come in the same form.[34] While some countries impose a blanket ban on the transfer of all personal data abroad, some, such as Australia, impose specific restrictions on data transfers in industries that require the possession of sensitive personal information such as the health and finance sectors.[35] Other countries, such as Malaysia and the Philippines, have enacted stringent consent requirements and regulatory approvals for data transfers.[36] This slows the data transfer process and often, in reality, results in forced data localization.[37]

The EU is starting to explore data localization as a means to further ensure the privacy of its citizens. In 2016, the EU adopted the General Data Protection Regulation (GDPR) to replace the Data Protection Directive (DPD).[38] Under the GDPR, the EU limited the transfer of personal data of EU citizens outside the EU to only those countries that had the same level of data protection as the EU.[39] While the EU emphasized that it was crucial to protect the privacy interests of its citizens, it also recognized the importance of free flow of data in commercial activity.[40] In response, the EU carved out certain exceptions to ensure that commercial activity requiring cross-border data flows could continue. The EU-U.S. Privacy Shield Framework, for instance, was created to allow more than 5,300 U.S. companies to transfer personal data necessary to conduct trade so long as certain criteria were met.[41]

However, in July 2020, the Court of Justice of the European Union ("CJEU") decision in *Data Protection Commission vs. Facebook Ireland, Max Schrems* (*Schrems II*) invalidated the Privacy Shield, which originally legalized most personal data flows from the EU to the U.S.[42] As a result, companies had to either stop the transfers immediately or find another lawful basis for them.[43] The remaining two legal options for data transfers under the GDPR, Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCRs), now require companies relying on those mechanisms to verify, "on a case-by-case basis, whether recipient countries offer a level of protection equivalent to EU law with

34. Mishra, *supra* note 32, at 139.

35. *Id*. at 11.

36. Chander & Lê, *supra* note 6, at 712; Mishra, *supra* note 32, at 139–40

37. Mishra, *supra* note 32, at 140.

38. Chris Mirasola, *Summary: The EU General Data Protection Regulation*, LAWFARE (Mar. 1, 2018), https://www.lawfareblog.com/summary-eu-general-data-protection-regulation [https://perma.cc/SN38-P9LN].

39. David Vance Lucas, *Schrems II, Part 2 - Additional Guidance for the Transfer of Personal Data Between the EU and the U.S.,* JD SUPRA (Sep. 10, 2020), https://www.jdsupra.com/legalnews/schrems-ii-part-2-additional-guidance-13869/ [https://perma.cc/VM9C-3SWK].

40. Mirasola, *supra* note 38.

41. Natasha Lomas, *EU-US Privacy Shield is Dead. Long Live Privacy Shield,* TECHCRUNCH (Aug. 11, 2020), https://techcrunch.com/2020/08/11/eu-us-privacy-shield-is-dead-long-live-privacy-shield/ [https://perma.cc/3MCX-G92C].

42. *Id.;* Case C-311/18, Data Prot. Comm'n v. Facebook Ireland (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020).

43. *Id*. at ¶ 5.

respect to government access to data."[44] If the legal protections of the recipient country do not meet EU standards, then companies must provide appropriate safeguards or refrain from transmitting the data.[45] This will likely make data transfers more difficult because few, if any, companies "possess the legal expertise and resources to perform such evaluations with regard to either U.S. law or the laws of other countries around the world."[46]

While the *Schrems II* decision never explicitly calls for data localization, companies may nevertheless be forced to localize their data in the EU to avoid the problems the decision raises.[47] While the ultimate results of *Schrems II* have yet to unfold, this decision and other policy decisions the EU made over the last few years indicate that it may continue to enact policies that favor data localization in the future.[48] Continued data localization in the EU would likely create more problems, such as driving up the cost of doing business, causing other nations to retaliate, and hurting businesses that cannot afford to comply with EU privacy regulations.[49]

In general, there is debate over the effectiveness of data localization as a means of protecting privacy. Some academics argue that efforts to strengthen privacy through localization may have the opposite effect.[50] For example, localized data servers reduce the opportunity to distribute information "across multiple servers in different locations."[51] More specifically, it significantly more difficult for companies to take advantage of mechanisms such as "sharding," which could further protect the privacy of individuals.[52] As a result, information gathered in a single

---

44. Bradley A. Booker, Sujit Raman & James M. Sullivan, *The Need for Clarity After Schrems II*, LAWFARE, (Sep. 29, 2020), https://www.lawfareblog.com/need-clarity-after-schrems-ii [https://perma.cc/K392-5TDB].

45. *Id.*

46. *Id.*

47. Anupam Chander, *Is Data Localization a Solution for Schrems II?* 23 J. INT'L ECON. L 771, 777 (2020).

48. The possibility of strict data localization has become greater after the European Data Protection Board (EPDB) released two documents (Recommendations 01/2020 and 02/2020) on November 10, 2020, following the *Schrems II* decision. The recommendations, though unclear, may mean that personal data cannot be transferred to data controllers or processors outside of the European Economic Area who require unencrypted access to personal data. Critics, such as Professor Theodore Christakis, have commented that the EDPB documents seem "to prohibit almost all [data transfers] when the personal data is readable in [a] third country." If European data has no way of leaving Europe (that is, in a readable format) that means it needs to remain in Europe. That, in essence, would be considered data localization. Peter Swire, *After Schrems II and the EDPB Guidance, Lessons from a 1998 Study About the Effects of Data Localization Between the EU and the US,* CROSS-BORDER DATA F. (Nov. 30, 2020), https://www.crossborderdataforum.org/after-schrems-ii-and-the-edpb-guidance-lessons-from-a-1998-study-about-the-effects-of-data-localization-between-the-eu-and-the-us/ [https://perma.cc/K3HC-424T].

49. Chander, *supra* note 47, at 782–84.

50. Chander & Lê, *supra* note 6, at 719.

51. *Id.*

52. *Id.* Sharding is the process in which rows of a database table are held separately in servers across the world - making each partition a "shard" that provides enough data for the operation of a system but not enough to re-identify an individual.

location can actually be a "tempting jackpot," offering an ideal target for foreign adversaries or criminals.[53]

C. DIGITAL PROTECTIONISM

Since traditional trade-protectionism tools, such as tariffs, are not as feasible when applied to the digital economy, some countries are "reverting to 'behind-the-border' regulations and technical requirements, such as data localization" to protect domestic economic interests.[54] These countries, often developing ones, believe that data localization measures are a mechanism to coerce high-tech economic activities to take place within their borders rather than to flow overseas.[55] Policymakers reason that if they restrict data flows, their countries will gain a net economic advantage from companies that will be forced to relocate data-related jobs to their nations.[56] They also believe that data localization measures are "powerful protectionist tools" that can help domestic digital firms catch up with leading multi-national firms.[57] For example, in 2012, Indonesia introduced broad-reaching data localization measures requiring service providers providing "public services" to place their data centers within the country.[58] Under the provision, a wide variety of industries, including "hotels, banks, airline services, as well as [Google and Yahoo] would be obligated to put data centers in Indonesian territory."[59] The provision was part of a broader government strategy to create greater employment, upgrade skills, and improve the economy.[60]

In theory, these protectionist measures offer the possibility for countries to foster economic growth[61] and are therefore politically appealing to the citizenry of those countries.[62] However, despite the perceived advantages of data localization, in practice, the actual efficacy of the requirements is minimal. In fact, data localization requirements aimed at protecting domestic companies and industries can actually backfire. For example, startups in developing countries such as Indonesia and Vietnam have often turned to foreign countries such as the United States, Singapore, and Australia to host their servers because many of the tools these startups relied on were not fully available in their own countries.[63] These

53. *Id.*

54. CORY, *supra* note 2, at 5.

55. *See id.*

56. INFO. TECH. & INNOVATION FOUND., NIGEL CORY, THE FALSE APPEAL OF DATA NATIONALISM, WHY THE VALUE OF DATA COMES FROM HOW IT'S USED, NOT WHERE IT'S STORED (2019).

57. WILLIAM DRAKE, WORLD ECON. F., DATA LOCALIZATION AND BARRIERS TO CROSS-BORDER DATA FLOWS TOWARDS A MULTITRACK APPROACH 7 (2018), http://www3.weforum.org/docs/White_Paper_Data_Localization_Barriers_Cross-Border_Data_Flows_report_2018.pdf [https://perma.cc/M3WB-X2CG].

58. Chander & Lê, *supra* note 6, at 677.

59. *Id.* at 699.

60. Mishra, *supra* note 32, at 147.

61. *Id.*

62. *Id.* at 137.

63. Chander & Lê, *supra* note 6, at 725.

countries also possessed insufficient infrastructure that would result in slower loading times than if they used overseas servers.[64] As the governments attempted to protect domestic businesses through data localization measures, the requirements "effectively bar[red] start-ups from utilizing cheap and powerful platforms abroad" and potentially handicapped the country from "join[ing] the technology race."[65]

In sum, even if localization could lead "small gains for a few local enterprises and workers," it could simultaneously cause significant harm to the economy felt by small, medium, and large businesses who are denied access to global services because of localizations measures.[66]

D. PUBLIC MORALS OR PUBLIC ORDER

Some governments – for example, China, Iran, and Vietnam – claim that data localization measures are necessary to protect public morals or maintain public order within their countries.

In China, the Chinese Communist Party (CCP) adopted strict policies regarding information control by initiating the Golden Shield Project, more commonly known as the "Great Firewall of China."[67] The Great Firewall was designed to monitor and censor what can be seen through the Chinese online network by enabling the CCP to control international gateways, filter online content, and block access entirely to some of the most common websites on the public internet.[68] The CCP has justified its wide-reaching data localization measures as being necessary to ensure that online content circulated within China is in line with important public values and maintains public order within the country.[69]

Iran and Vietnam have followed China and imposed restrictions on political information circulated online for the purposes of maintaining public order. Therefore, any information prejudicial to "'national security, 'cultural values' or 'public order' is prohibited."[70] These kinds of regulations "have the net effect of preventing cross-border transfer of data from foreign countries" into Vietnam and Iran, where specific websites or types of content are banned.[71]

The countries that use the public morals and order as justification for their localization measures all have an interest in controlling what their citizenry can

---

64. Ross Settles, *Indonesia: A Hotbed of Innovative Online Publishing Start-ups*, CLICKZ (Mar. 30, 2011), http://www.clickz.com/clickz/column/2281593/indonesia-a-hotbed-of-innovative-online-publishing-startups [https://perma.cc/VS72-ASKY].

65. Chander & Lê, *supra* note 6, at 725.

66. *Id.*

67. *Free Speech vs. Maintaining Social Cohesion,* STANFORD UNIV., https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html [https://perma.cc/4TN8-ASW8].

68. Aaronson & Leblond, *supra* note 18, at 262.

69. Shahbaz et al., *supra* note 9.

70. Mitchell & Hepburn, *supra* note 12, at 191.

71. *Id.*

and cannot see.[72] These countries are often at odds with other countries that advocate for freer flow of data and even free speech. Stark differences in values and ideologies may make it extremely difficult to bridge the gap between those countries and may discourage the free flow of data between such regimes, which can cause both countries to fail to fully capture potential economic opportunity.

II. COSTS OF DATA LOCALIZATION

Several studies have highlighted the scale and importance of cross-border data flows.[73] These studies show that data's value is maximized when it can flow across companies and sectors, and that cross-border data flows add significant value to export growth, GDP, and job growth.[74] Data localization requirements, especially poorly conceived ones, can constrain the flow and use of data and simultaneously drive up costs of conducting businesses, hinder innovation, and further exacerbate inefficiencies broadly across the economy.[75] Although the tradeoffs of data localization are not generally understood or discussed in the current literature with regards to localization,[76] the next section explores some of the direct and indirect costs that result from localization measures.

A. INCREASED COSTS OF DOING BUSINESS AND RESULTING COMPETITION CONCERNS

Data localization measures have the potential to make conducting business significantly more expensive.[77] To comply with data localization measures, businesses could be forced to spend more money than necessary on IT and storage services to conduct business on foreign soil.[78] Additionally, companies may be compelled to spend more on compliance activities, such as hiring data-protection officers or putting in place software and systems to get individuals' or governments' approval to transfer data.[79] Such barriers could also make it more difficult

72. *See id.*

73. *See, e.g.*, GSMA, CROSS-BORDER DATA FLOWS: REALIZING BENEFITS AND REMOVING BARRIERS (2018), https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-diesputeremoving-barriers_Sept-2018.pdf [https://perma.cc/UF5K-WNB4]; Susan Lund & James Manyika, *Defending Digital Globalization,* MCKINSEY GLOB. INST. (Apr. 20, 2017), https://www.mckinsey.com/mgi/overview/in-the-news/defending-digital-globalization#:~:text=According%20to%20research%20we%20conducted,data%20flows%20%E2%80%9Cdigital%20globalization.%E2%80%9D [https://perma.cc/9SZR-M2WN]; INST. INT'L FINANCE, DATA LOCALIZATION: COSTS, TRADEOFFS, AND IMPACTS ACROSS THE ECONOMY (2020), https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf [https://perma.cc/W3E7-WZL9].

74. Meltzer & Lovelock, *supra* note 5.

75. INST. INT'L FINANCE, DATA LOCALIZATION: COSTS, TRADEOFFS, AND IMPACTS ACROSS THE ECONOMY 4–5 (2020), https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf [https://perma.cc/W3E7-WZL9].

76. *Id.* at 4.

77. CORY, *supra* note 2, at 6.

78. *Id.*

79. *Id.* at 7.

for companies to transfer data that is needed for day-to-day operations, which means that companies would likely have to purchase duplicative services.[80] The resulting additional costs ultimately could cut into profit margins, undermining a firm's competitiveness.

Currently, there is a scarcity of complete data sources that quantify the actual costs of data localization on businesses and economic growth. However, some previously published studies give some insight into what the costs of such measures would be.[81] One study published in 2015 by the Leviathan Security Group, focused on capturing the impact data localization measures would have on access to cloud services in Brazil and Europe if data localization measures cut these countries off from the most cost-competitive global cloud providers.[82] It found that if Brazil had enacted data localization as part of its "Internet Bill of Rights" in 2014, companies would have to pay an average of 54% more to use cloud services from local cloud providers compared with the lowest worldwide price.[83] The European Union, on the other hand, would have to pay up to 36% more.[84] Leviathan then concluded that for other countries considering data localization, local companies would be similarly required to pay up to about "30-60% more for their computing needs" than if they could go outside the country's borders.[85]

Additionally, in the long run, these increased costs can disproportionately hurt smaller and medium-sized enterprises (SMEs). At the moment, the global nature of the Internet allows SMEs to reach foreign markets they otherwise would not be able to.[86] A study conducted by eBay found that about 95% of U.S. SMEs sell products on its platform to foreign markets.[87] Policies that require data localization hurt these SMEs because they make it more difficult to expand into markets beyond their own country. SMEs often have neither the expertise nor budget to afford the mechanisms to store and protect data.[88] While larger enterprises can

---

80. *Id.* at 6.

81. *See e.g.,* MATTHIAS BAUER, HOSUK LEE-MAKIYAMA, ERIK VAN DER MAREL & BERT VERSCHELDE, EUROPEAN CTR. FOR INT'L POL. ECON., THE COSTS OF DATA LOCALIZATION: FRIENDLY FIRE ON ECONOMIC RECOVERY (May 2014); MATTHIAS BAUER, MARTINA F. FERRACANE & ERIK VAN DER MAREL, CTR. FOR INT'L GOVERNANCE INNOVATION, TRACING THE ECONOMIC IMPACT OF REGULATIONS ON THE FREE FLOW OF DATA AND DATA LOCALIZATION (May 2015).

82. LEVIATHAN SEC. GRP., QUANTIFYING THE COST OF FORCED LOCALIZATION 9–11 (2015), https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf [https://perma.cc/H4HN-PTZ3].

83. *Id.* at 9.

84. *Id.* at 10.

85. *Id.* at 3.

86. Cody Ankeny, *The Costs of Data Localization,* INFO. TECH. INDUS. COUNCIL (Aug 17, 2016), https://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization [https://perma.cc/GM92-SXGN].

87. EBAY PUB. POL'Y LAB, 2015 US SMALL BUSINESS GLOBAL GROWTH REPORT 6 (2015). https://www.ebaymainstreet.com/sites/default/files/2015-us-small-biz-global-growth-report_0.pdf [https://perma.cc/CSP4-8AZW].

88. Ankeny, *supra* note 86; WORLD ECON F., A ROADMAP FOR CROSS-BORDER DATA FLOWS: FUTURE-PROOFING READINESS AND COOPERATION IN THE NEW DATA ECONOMY 16 (2020).

more easily adapt to the localization demands implemented, SMEs are more likely to be pushed out of the market, thereby decreasing competition.

B. HINDRANCE TO INNOVATION

Businesses and other organizations collect and synthesize data to generate insights, which leads to innovation.[89] Data collected by businesses are often used to enhance research and development, develop new products, improve marketing, and establish organizational and management approaches.[90] Data localization laws could result in delays and higher costs in the development of new and innovative goods because companies may be hindered from accessing the data of their preferred research partners.[91] At the same time, countries that enact data flow barriers make it more expensive for both domestic and foreign entities to gain exposure and benefit from ideas, research, technologies, and best practices making them less competitive on the global front.[92] As a result, countries who choose to localize data as part of an effort to bolster their domestic industries may see the opposite effect manifest.

C. INCREASED RISK FOR INTERNET BALKANIZATION

One major concern regarding data localization laws is that such policies are likely to balkanize the Internet, fragmenting the global network into "various distinct, idiosyncratic '(I)nternets'" which would result in delays, inefficiencies, and higher costs.[93] If data localization requirements become widespread, businesses active in the global digital economy would likely have to navigate a "complex array of different jurisdictions imposing conflicting mandates and conferring conflicting rights."[94] Companies may then be discouraged from investing in local infrastructure in developing countries, leaving gaps in Internet service in those countries.[95] This could, in turn, jeopardize the benefits individual users and businesses enjoy from integrated global communications and the digital economy.

An additional concern is that as various regions demand data localization requirements from foreign and local companies, other countries may respond in kind and erect retaliatory barriers, harming consumers and limiting domestic companies' abilities to expand globally via the Internet.

---

89. CORY, *supra* note 2, at 7.

90. *Id.* at 1.

91. *Id.* at 7.

92. Erica Fraser, *Data Localization and the Balkanization of the Internet,* 13 SCRIPTED 360, 368 (2016), https://script-ed.org/wp-content/uploads/2016/12/13-3-fraser.pdf?d=11222020 [https://perma.cc/9GBB-MBAR].

93. *Id.* at 362 (quoting Sascha Meinrath, *We Can't Let the Internet Become Balkanized,* SLATE (Oct 14, 2014), http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html [https://perma.cc/EX52-2932]).

94. *Id.* at 362 (quoting Meinrath, *supra* note 93).

95. *Id.*

III. ADEQUACY OF THE WTO IN SAFEGUARDING AGAINST EXCESSIVE DATA LOCALIZATION MEASURES

As established in Parts I and II of this paper, data localization laws can result in significant costs and minimal benefits. Given the increasing importance of cross-border data flows in economic growth and the huge costs that come with attempting to limit those flows, it is important to create solutions that strike a balance between governmental autonomy in managing legitimate risks and data liberalization. The key challenge will be to find solutions that enable the freer flow of data between countries that have different philosophies, values, and objectives with regards to data.

The use of the WTO is a potential solution to prevent excessive data localization measures. The following sections will evaluate whether the WTO is adequate in regulating cross-border data flows and in preventing excessive data localization measures.

A. CROSS-BORDER DATA FLOWS UNDER THE GENERAL AGREEMENT ON TRADE IN SERVICES ("GATS")

Before evaluating whether the WTO is adequate in addressing data localization issues, it is important to determine whether cross-border data flows, as a whole, can be assessed under available WTO frameworks. The existing WTO laws largely predate the proliferation of the digital economy and data transactions.[96] However, since 2018, the WTO has had several agreements that implicitly relate to digital trade as a whole.[97] Of the agreements, the GATS is likely the most applicable framework to cross-border data flows and data localization measures.[98] The GATS applies to the supply of services, including the production distribution market sale, and delivery of services.[99] It does not require the physical presence of one Member country's supplier in another Member's territory and therefore includes trade in digital services.[100] The cross-border supply of digital services

96. John A. Drennan, J, Michael Taylor, Joseph Laroski, Alexander K. Haas & Jule A. Stockton, *Privacy Law, Cross-Border Data Flows, and the Trans-Pacific Partnership Agreement: What Counsel Need to Know*, BLOOMBERG PRIVACY & SECURITY LAW REPORT (Dec 2015).

97. Mitchell & Hepburn, *supra* note 12, at 186–87; MARK WU, INT'L CTR. FOR TRADE & SUSTAINABLE DEV., DIGITAL TRADE-RELATED PROVISIONS IN REGIONAL TRADE AGREEMENTS: EXISTING MODELS AND LESSONS FOR THE MULTILATERAL TRADE SYSTEM 1 (2017).

98. To see full analysis as to why GATS is the applicable WTO rule system, please refer to DANIEL CROSBY, E15 INITIATIVE, ANALYSIS OF DATA LOCALIZATION MEASURES UNDER WTO SERVICES TRADE RULES AND COMMITMENTS 2 (Mar. 2016), http://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf [https://perma.cc/D5XE-K4RH].

99. General Agreement on Trade in Services art. 28(b), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 189 [hereinafter GATS].

100. These include the Information Technology Agreement (which eliminates duties for trade in computer and information technology equipment), the Agreement on Trade-Related Aspects of IP Rights (which protects trade-related IP pertinent to information technology), the General Agreement on Tariffs and Trade (which relates to digital goods, like software or music in electronic format, embedded in physical medium), and the General Agreement on Trades and Services.

inevitably includes cross-border data flows. As such, data localization measures that restrict cross-border data flows can fall under the scope of GATS.

B. WTO'S EFFECTIVENESS IN PREVENTING DATA LOCALIZATION MEASURES

While the rules of the WTO (particularly under the GATS) likely cover cross-border data flows, it is limited in its ability to provide safeguards and regulate against excessive data localization measures. The following sections explore the reason why the GATS and WTO as a whole are minimally effective in achieving those endeavors.

1. THE APPLICATION OF THE ARTICLE XVII: NATIONAL TREATMENT AND ARTICLE XVI:2 MARKET ACCESS PROVISIONS IS QUESTIONABLE

Several provisions of the GATS may apply to data localization measures.[101] Article 27 of GATS, the national treatment provision, for example, provides that Members have to accord services and service suppliers of any other Member "treatment no less favourable than that it accords to its own like service and service suppliers" and applies to all sectors where specific commitments have been undertaken.[102] If a specific data localization measure affects the supply of a service in a sector in which a Member has specific commitments, then the measure may violate its national treatment obligation.[103] This is because the data localization measure could cause a foreign firm to expend significant resources to comply, making it more difficult for the firm to remain competitive or have to forgo entering into the domestic market altogether.[104]

GATS Article 16(2), the market access provision, may also apply. Under this provision, if a Member lists a particular sector on its Schedule of Specific Commitments, then it shall not adopt measures which impose "limitations on the number of service suppliers whether in the form of numerical quotas, monopolies, exclusive service suppliers, or the requirements of an economic needs test."[105] Applying this rule, it is arguable that a data localization measure is a limitation on the number of service suppliers as it prevents the use of service suppliers of one, several, or all means of delivery of cross-border digital service.[106]

The problem with using these provisions to safeguard against data localization measures is that applying them would require interpretation as to whether the data transfers being hindered by localization were sufficiently related to certain sectors in which members have commitments. For example, in the past, when the EU and other WTO members have attempted to enact certain data restrictive

101. Wong, *supra* note 7, at 161.
102. CROSBY, *supra* note 98, at 8.
103. *See* Wong, *supra* note 7, at 161.
104. *Id*.
105. GATS, *supra* note 99, at art. 16(2)(a).
106. Mitchell & Hepburn, *supra* note 12, at 200–01.

measures on particular digital service industries, to justify their policies they have often relied on a service classification loophole.[107] They would argue that the digital services they were restricting should be classified under the "audiovisual services" sector instead of another sector, such as "computer services," because of their inherent function as content platforms.[108] This is because almost no WTO members have made any commitments under the audiovisual services sector (as opposed to the computer services sector).[109] Thus, if member states could successfully classify the services under the audio services sector, they would remain free to sustain and adopt new discriminatory measures.[110]

Unfortunately, since the GATS classification system predated the proliferation of the Internet and has not kept pace with technological developments, it is relatively easy for member states to classify services into sectors in which there is little commitment and would thereby allot more room for member states to implement restrictive policies.[111] These kinds of uncertainties regarding classification may need to await clarification on a case-by-case basis given the lack of precedent put forth by the WTO Appellate Body. Without more guidance, the application of the GATS provisions and the effectiveness in preventing overreaching data localization measures remains unclear.

2. THE SCOPE OF THE GATS XIV EXCEPTIONS IS AMBIGUOUS

Even if substantive violations of the GATS provisions might arise, countries that choose to localize their data could justify such policies under the general and security exceptions of Article XIV and Article XIV*bis,* respectively.[112] These exceptions allow countries to derogate from their trade liberalization commitments based on specified public policy objectives.[113] However, there is only modest guidance as to the scope of these exceptions. This means that if countries choose to implement data localization measures, they may, with relative ease, cite a rationale that falls within the GATS exceptions, making it more difficult to prevent excessive data localization measures.

Take, for example, Article XIV(a), which allows Member states to forgo their GATS obligations when they are "necessary to protect public morals or to maintain public order."[114] Public morals in this context "denotes standards of right and wrong conduct maintained by or on behalf of the community or nation."[115] WTO

107. Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C. DAVIS L. REV. 65, 85 (2017).

108. *Id*.

109. *Id*. at 85–86.

110. *Id*. at 86.

111. Michell & Hepburn, *supra* note 12, at 198.

112. Hodson, *supra* note 1, at 579–80.

113. Wong, *supra* note 7, at 161–62.

114. GATS, *supra* note 99, at art. 14(a).

115. World Trade Org., *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, at ¶ 7.759, WTO Doc. WT/DS363/R (Aug. 12, 2009).

tribunals have historically given considerable deference to governments to define what they consider to be public morals and the measures they take to achieve such means.[116] This gives ample room for countries to implement data localization measures that are arguably designed to repress speech and political opposition while citing public morals as a cover and justification for such severe measures. For example, Chinas has created laws and policies to ensure that all content that is circulated within the country is in line with its public values.[117] As a result, websites such as Facebook are banned from entering Chinese borders.[118]

The scope of the Article XIV*bis* national security exception is also ambiguous. Under XIV*bis,* a country can deviate from its WTO obligations for "the protection of its essential security interests" under certain circumstances[119] such as during "time[s] of war or in other emergency in international relations."[120] Here, for example, it is unclear whether the term "emergency" could refer to new arising situations that are not traditionally considered "war," such as cyberwarfare, civil uprisings, and bioterrorism. Additionally, neither the WTO panel nor the Appellate Body has opined on the scope of the GATS national security exception, further compounding the ambiguity.[121] As a result, given the seemingly "self-deciding" nature of the provision, it is extremely difficult to determine the limits of the exception, paving the way for a country to possibly deem data localization a necessary component of its national security protection efforts.

3. RELYING ON THE APPELLATE BODY TO RESOLVE GATS AMBIGUITIES

The absence of rules pertaining directly to data localization and the ambiguity of the current scope of the WTO provisions and exceptions can make it difficult for Member states, which have different sentiments towards data localization, to come to a consensus. Any clarification on the WTO rules regarding data localization would likely have to be decided by the Dispute Settlement Bodies ("DSB") Panels or the Appellate Body.[122] However, there are several drawbacks to relying on such bodies.

First, the judges and panelists assigned to the WTO Bodies may define the scope of the WTO rules in relation to data localization in a way that is not representative of the view of Member states.[123] This could increase jurisdictional conflict over interpretation of the provisions and exceptions, leading to further

116. *See e.g.,* Appellate Body Report, *China – Publications and Audiovisual Entertainment Products,* WTO Doc. WT/DS363/AB/R (adopted Dec. 21, 2009) [hereinafter *China – Publications and Audiovisual Products];* Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services,* WTO Doc. WT/DS284/AB/R (adopted Apr. 7, 2005) [hereinafter *US– Gambling*].

117. Mitchell & Hepburn, *supra* note 12, at 190.

118. *Id*. at 191.

119. GATS, supra note 99, at art. 14*bis*(1)(b).

120. GATS, supra note 100, at art. 14*bis*(1)(b)(iii).

121. Roger P. Alford, *The Self-Judging WTO Security Exception,* 3 UTAH L. REV. 697, 707 (2011).

122. *See* Mitchell & Hepburn, *supra* note 12, at 195.

123. Hodson, *supra* note 1, at 582.

divergence and distrust amongst the member states. Second, even if the WTO Bodies rendered decisions to help define the scope of provisions and exceptions, the WTO Bodies lack the "teeth" to enforce those measures. Members who oppose the WTO interpretations can exercise a tactic called "uncompliance" in which a Members formally comply with the rules but adopt other measures that have equivalent protectionist effects that essentially invalidate the ruling's impact.[124] Although data localization measures have not been formally adjudicated under the WTO Bodies, this tactic has been used in the past.[125]

China, for example, has been accused of using such methodologies to blunt the intrusiveness of WTO holdings. In 2007, the United States challenged various aspects of China's IP regulatory scheme through *Protection and Enforcement of IPR (DSB 362)*.[126] The Appellate Body found that China's customs regulation, which allowed counterfeit goods to re-enter the stream of commerce once the infringing elements had been removed, violated the Trade-Related Aspects of Intellectual Property ("TRIPS"). In response, the Chinese State Council revised its laws in a way that seemed to prevent counterfeit goods from reentering channels of commerce, and thus addressed the U.S.'s concerns.[127] However, upon closer look, the law only applied to imported counterfeit goods, which are goods produced outside of China.[128] The qualifier "imported" narrowed the scope and applicability of the law; China, the largest producer of counterfeit goods, would remain untouched by the revision of the law.

The WTO's weak remedy system and disciplinary measures for non-compliance make it difficult for Appellate Body rulings to change any behaviors, as demonstrated by China's actions after the *Protection and Enforcement of IPR* decision. Consequently, countries wishing to maintain stringent data localization laws even after a future WTO Appellate Body decision is rendered may utilize these "uncompliance" tactics to superficially comply with the WTO law while maintaining tight control over their data flows.

4. WTO LACKS THE EXPEDIENCY TO ADJUST TO A QUICKLY CHANGING DIGITAL ECONOMY

Lastly, the WTO is unlikely to modify its rules at a sufficient pace to keep up with the rapidly changing digital economy. To make substantive changes or to expand the scope of current WTO rules, member states must reach a consensus

124. Gregory Shaffer, Manfred Elsig & Sergio Puig, *The Extensive (But Fragile) Authority of the WTO Appellate Body,* 79 L. & CONTEMP. PROBS. 237, 269–70 (2016).

125. *See* Timothy Webster, *Paper Compliance: How China Implements WTO Decisions,* 35 MICH. J. INT'L L. 525, 533–35.

126. For more detail of the case, *see id*. at 557–62.

127. *Id*. at 560.

128. *Id*.

on data flow principles.[129] This is very unlikely to occur because while some countries have an interest in complete data liberalization, others do not.[130] Coming to an agreement in a consensus-based system would be extremely difficult to do. Furthermore, the WTO has historically been notoriously slow at reacting to technological changes. For example, as early as 1998, governments recognized the need to clarify the relationship between trade rules and emerging online modes of trade.[131] The WTO Work Programme on Electronic Commerce was designated with the task of exploring WTO rules and the production, distribution, marketing, sale, or delivery of goods and services by electronic means.[132] Even so, attempts to update the digital trade rules at the multilateral level have stalled.[133] At the same time, data localization measures are rapidly increasing. In 2019 alone, India, Indonesia, and Vietnam all introduced laws requiring personal or business data to be kept within national borders.[134] Additionally, the rise of new technologies, including AI and cloud-based computing, will lead to an increasing number of connected devices and data, presenting new and unanticipated challenges to data regulation as well.[135]

While the WTO was designed to be technologically neutral and therefore flexible,[136] it is unlikely that any necessary changes to the WTO provisions and rules to adapt to the realities of our digital economy today will be achieved quickly enough to singlehandedly prevent continued localization.

IV. ALTERNATIVE WAYS TO ADDRESS DATA LOCALIZATION MEASURES AND HOW THE LEGAL PROFESSION CAN HELP

In light of the potentially devastating consequences that result from continued data localization, it is pertinent to develop solutions independent of the current use of WTO roles that would encourage the free flow of data while simultaneously allowing governments to effectively achieve their public policy goals. As mentioned in the previous sections, excessive data localization measures cannot simply be overcome by utilizing the WTO as a one-stop shop solution. As a result, a constellation of solutions would be needed to regulate the free flow of

129. Jack Caporal, Dylan Gerstel & Matthew Sullivan, *WTO Reform: The Beginning of the End or the End of the Beginning?* CTR. FOR STRATEGIC & INT'L STUDIES (Oct. 23, 2018), https://www.csis.org/analysis/wto-reform-beginning-end-or-end-beginning [https://perma.cc/R7CA-M97T].

130. *See* Aaronson & Leblond, *supra* note 18, at 253–68.

131. WU, *supra* note 97, at 1.

132. *Id.*

133. *Id.*

134. *Internet Way of Networking Use Case: Data Localization,* INTERNET SOC'Y (Sep. 13, 2020), https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/ [https://perma.cc/U6LD-8VXJ].

135. Jennifer Huddleston & Jacqueline Varas, *Impact of Data Localization Requirements on Commerce and Innovation*, AM. ACTION F. (June 16, 2020), https://www.americanactionforum.org/insight/impact-of-data-localization-requirements-on-commerce-and-innovation/#ixzz6en98n5Dy [https://perma.cc/E3AW-H2CA].

136. *See US –Gambling.*

data. The next sections discuss potential solutions that can be taken to help regulate the free flow of data, as well as how the legal profession can play a role in developing these solutions.

A. SOLUTIONS ON THE INTERNATIONAL FRONT

1. ESTABLISH A SEPARATE FRAMEWORK FOR DATA FLOWS THROUGH INTER-GOVERNMENTAL FORUMS

As mentioned in Part I, there are numerous data regimes throughout the world, some of which are seemingly incompatible. This is often reflective of countries' divergent values, interests, and attitudes toward the free flow of data. At the moment, no complete and robust international framework governing the free flow of data exists.[137] Given the variety of interests that motivate governments to implement data localization measures, it may prove difficult to immediately create a global data flow obligation amongst countries through the WTO, which requires consensus-based decision making. However, a good starting point would be for various nations to come together to establish a data flow framework outside the WTO that could provide guidance to cross-border data flow related issues. A potential framework could include a) aspirational data flow principles that countries will strive to attain and uphold and b) a standardized process that countries can use to conduct cost-benefit analysis for proposed data localization measures.

a. Establish Aspirational Data Principles

First, the framework should include a set of aspirational data principles that countries agree to strive for. Here, government officials, companies, academics, and technology experts could come together to create baseline principles that could encourage the free flow of data and discourage excessive data localization measures. One principle, for instance, could be that countries must endeavor to facilitate the free flow of data across borders and to avoid data localization measures that do not assist countries in reaching their legitimate public policy goals.

The Asia-Pacific Economic Cooperation ("APEC") Privacy Framework is an example of a principles-based model used to guide cross-border data flows of personal information.[138] Created in 2005, the Privacy Framework aimed to "balance[] information privacy and business need and commercial interests, and at the same time, accord[] due recognition to cultural and other diversities that exist within member economies."[139] Consequently, it presented nine guiding

137. There are some trade agreements and regional frameworks that have been developed to address the cross-border data transfers. However, a global framework that helps to establish obligations, standards, and best practices with regards to cross-border data flows has not been developed.

138. Carla Bulford, *Between East and West: The APEC Privacy Framework and the Balance of International Data Flows,* 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 705, 705 (2007).

139. APEC SECRETARIAT, APEC PRIVACY FRAMEWORK 3 (2005), https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework [https://perma.cc/GD3C-S3WY].

principles[140] that could be used both by member states to adopt comprehensive privacy legislation and by industry groups and individual companies to implement self-regulatory standards.[141] The framework also provided guidance on how the nine APEC Privacy Principles could be implemented.[142]

The new framework could model itself after the APEC framework. It could establish both aspirational principles that encourage the free flow of data and discourage excessive data localization measures and implement guidelines to help shape countries' data flow policies. The creation of the framework would be crucial for establishing trust amongst nations because it would provide basic standards that all must adhere to. Here, lawyers can play a substantial role in helping develop the principle-based framework by participating in its initial development. The ABA Commission on Ethics 20/20 was created in August 2009 to study the impact of technology and globalization.[143] As part of its process, the Committee actively "held hearings, considered a wide range of issues, had representatives from a range of ABA and outside entities participate in the development of its work product, circulated discussion papers, and even participated in 'outreach events.'"[144] In the end, by August 2012, the Commission presented six resolutions related to the development of technology and globalization.[145] All six were adopted by the ABA House of Delegates.[146] Similarly, lawyers can utilize a similar process – they can facilitate discussions between representatives of various nations and review established data ethics frameworks to analyze common elements and themes amongst data policy of various countries to inform development of a data flow framework. Lawyers can then work with other stakeholders, such as technology experts and economists, to help design and assess the effectiveness of the framework.

b. Create Standardized Process to Conduct Cost-Benefit Analysis of Data Localization Measures

As observed in Parts I and II of this paper, at the moment, there is limited research available that weighs the real cost and benefits of data localization

140. The nine principles are: preventing harm, notice, collections limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability.

141. Bulford, *supra* note 138, at 705.

142. APEC SECRETARIAT, *supra* note 139, at 30–36.

143. COMM'N ON ETHICS 20/20, AM. BAR ASSOC., INTRODUCTION & OVERVIEW 1 (2012), https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20121112_ethics_20_20_overarching_report_final_with_disclaimer.pdf [https://perma.cc/ST68-QE33].

144. *Id*.

145. *Id*. The topics addressed in these six resolutions were: Technology and Confidentiality; Technology and Client Development; Outsourcing; Practice Pending Admission; Admission by Motion; and Model Rule 1.6: Detection of Conflict of Interest.

146. *Id*. at 98.

measures.[147] Without enough information, it is very difficult to determine whether a set of data localization measures is effective and appropriate. The new data flow framework could also include a standardized process for conducting cost-benefit analysis on data localization measures that are introduced in the future.

The cost-benefit methodology for evaluating data localization measures can be modeled after other assessment processes currently used to evaluate regulation. The United States, for example, has a robust assessment process, known as the Environmental Impact Assessment (EIA), used to evaluate the impact proposed federal programs, policies, or legislation will have on its surrounding environment.[148] Under the National Environmental Policy Act, when an agency proposes a new project, it is required to conduct an EIA and publish an Environmental Impact Statement (EIS) that discusses the environmental impact of the proposed project, any unavoidable adverse environmental impacts from the proposal, the relationship between local short-term uses of person's environment and the maintenance and enhancement of long-term productivity and any irreversible commitments of resources that the proposed action would require.[149] Additionally, agencies must offer alternatives to the proposed project.[150] After the EIS is completed, agencies with jurisdiction comment on issues in the EIS.[151] The public also has the opportunity to comment during this period.[152] After the commenting period is over, the agency must respond to the comments, make proper changes to the EIS, and announce a revised proposed action.[153] Once all of that is done, the project is allowed to proceed.[154]

Similarly, the data flow framework can establish a process that countries must use to evaluate the impact of their proposed data localization measures. For example, the process could require that countries that wish to implement data localization measures submit an impact statement that discusses actual benefits, monetary costs, and alternatives to the proposed measures.[155] Once the impact statement is submitted, member states can evaluate and express concerns that they have with regards to the localization measure. Subsequently, countries can make the proper adjustments to their proposals until it receives approval by member states.

---

147. Although this paper cites to some studies that discuss the costs and benefits of data localization measures, the conclusions remain somewhat speculative.

148. CTR. FOR INT'L ENV'T L., A COMPARISON OF SIX ENVIRONMENTAL IMPACT ASSESSMENT REGIMES 1 (1995).

149. *Id*. at 17.

150. *Id*. at 6.

151. *Id*. at 24.

152. *Id*.

153. TIFFANY MIDDLETON, AM. BAR. ASSOC., WHAT IS AN ENVIRONMENTAL IMPACT STATEMENT? (2018).

154. *Id*.

155. The framework could also introduce a standardized way of evaluating the costs and benefits of localization measures.

Establishing a process for countries to follow can help facilitate informed and transparent decision-making while seeking to avoid, reduce, or mitigate potential adverse impacts. An established process would allow countries who wish to localize to more clearly evaluate just how effective their proposed measures would be. In turn, countries would be more likely to implement data restrictive measures that are actually beneficial and more easily avoid excessive costs.

2. UTILIZE A DIVERSE SET OF STAKEHOLDERS, INCLUDING LAWYERS, TO FINETUNE DISPUTE SETTLEMENT SYSTEM'S ABILITY TO ASSESS LEGALITY OF DATA RESTRICTIVE MEASURES

Even if a data flow framework is established, disputes regarding the legitimacy of the reasons behind enacted data localization measures will inevitably arise. As such, a dispute settlement system must be created[156] to resolve conflicts of interpretation. The dispute settlement system must be equipped with the following: 1) benchmarks and standards to help determine the legitimacy of certain data localization measures, and 2) tribunals with enforcement mechanisms to ensure that countries abide by the tribunal holdings.

To establish the first requirement, dispute systems will have to involve multiple stakeholders to help establish standards to evaluate data localization measures. As seen with the WTO Appellate Body, tribunals typically have "considerable discretion in assessing the legality of a data transfer-restrictive measure."[157] However, as described by Mitchell and Hepburn, tribunals "may lack the requisite knowledge of foundational issues such as the efficacy of technical standards on security and privacy, the economic impact of data transfer restrictions, and the technical feasibility and reliability of proposed alternative measures."[158] To strengthen the dispute settlement system, standards and frameworks must be created so that courts can more successfully balance data flow liberalization objectives with public policy goals and develop future jurisprudence. Multiple stakeholders, such as lawyers, economists, and technical experts, assist the courts in deciding which factors to take into account when faced with data localization disputes. These stakeholders can contribute to the finetuning of data localization standards utilized by the court, by playing an advisory role or having lawyers bring challenges before the court to help shape data localization jurisprudence.

This multi-stakeholder approach has been utilized before in the context of internet governance. In 2012, the South Korean Constitutional Court unanimously held that certain user identity verification provisions in the country were

---

156. I suggest a new dispute settlement system because WTO DSB functionality has stalled. Emre Peker, *'The WTO is in Crisis' : Dispute Puts Global Trade Regulator at Risk*, WALL ST. J. (Dec. 9, 2019), https://www.wsj.com/articles/the-wto-is-in-crisis-dispute-puts-global-trade-regulator-at-risk-11575889201 [https://perma.cc/U72U-34XN].

157. Mitchell & Hepburn, *supra* note 12, at 231.

158. *Id*. at 232.

unconstitutional.[159] The Court reached the decision after certain South Korean Internet stakeholders—including academics, the business community, technical community, civil society, and lawyers who were heavily involved in internet governance discussions—challenged the identity verification provisions.[160] The lawyers designed a litigation framework and gathered input, examples, rationale, and research from different stakeholders to submit to the court. The stakeholders each contributed unique information; for example, the technical community provided information about how futile, technologically, the verification process was.[161] In the end, the Constitutional Court issued a unanimous ruling citing many of the economic consequences, privacy implications, and free speech issues the stakeholders presented as part of its decision.[162] While the case in South Korea was an example of reactive multi-stakeholder collaboration, the same concept can be applied to data flow governance. Stakeholders involved with data flow governance can utilize their expertise to shape the international law and standards in this area.

In addition to being equipped with proper standards and frameworks to make decisions regarding data flow governance, a dispute settlement system must also be equipped with the ability to enforce measures. For example, an enforcement mechanism could allow prevailing parties to respond accordingly if offending members fail to change their policies. Other enforcement mechanisms could include monetary fines for countries that fail to comply.

Overall, by establishing enforcement mechanisms and standards and frameworks that the dispute settlement court can use, there would likely be less legal ambiguity, therefore increasing the legitimacy of the system. Countries would be able to rely on a dispute resolution system that produces fair and enforceable results. As a result, countries may develop trust in the international bodies to be able to protect their interests, therefore discouraging them from resorting to data localization measures.

B. SOLUTIONS ON THE DOMESTIC FRONT & THE ROLE OF THE LEGAL PROFESSION

Given our increasingly globalized world, it is likely that domestic policies must change as data flows on the international front change. [163] For example, as Europe continues to change its data privacy policies and moves towards favoring

159. ANRI VAN DER SPUY, WHAT IF WE ALL GOVERNED THE INTERNET? ADVANCING MULTISTAKEHOLDER PARTICIPATION IN INTERNET GOVERNANCE 51–52 (2017). For five years, provisions had required all major website operators in the Republic of South Korea to obtain, verify, and store personal identification details from any user wanting to post anything on their platforms. *Id.*

160. *Id.* at 55–56.

161. *Id.*

162. *Id.* at 56.

163. *See* William W. Burke-White & Anne-Marie Slaughter, *The Future of International Law is Domestic (or, The European Way of Law)*, 47 HARV. INT'L L.J. 327, 328 (2006).

data localization, the U.S. government and other industries would likely have to alter best practices to avoid enormous fees resulting from noncompliance. While lawyers on the international stage can help shape principles and norms in order to curb data localization measures and help facilitate the free flow of data, lawyers can play a role on the domestic front as well, by helping 1) industries adjust their practices to comply with changing domestic and international laws and minimize risk and 2) providing guidance for other lawyers on how to navigate changing data flow regulation. For the purposes of this section, I will focus on lawyers and the broader legal community in the United States.

1. LAWYERS CAN HELP COMPANIES ADJUST THEIR PRACTICES TO COMPLY WITH CHANGING DATA LAWS

As laws regarding cross-border data flows continue to change, lawyers will likely have to play an increasingly large role in helping clients (often domestic businesses) identify and understand their data obligations and devise solutions to meet them.[164] Rule 2.1 of the ABA *Model Rules of Professional Conduct* states that lawyers can serve as advisors to their clients.[165] When doing so, lawyers "shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to the law but to other considerations such as moral, economic, social, and political factors that may be relevant to the client's situation."[166] As a result, lawyers may not only be responsible for helping ensure that its clients comply with the technicalities of data flow laws, but also help companies mitigate potential risks and develop tools to make decisions regarding data. For example, lawyers can help their clients create corporate data policies that are sensible, logical, and compliant with industry standards, but also aligning with the values of the company.

2. THE BROADER LEGAL COMMUNITY CAN PROVIDE GUIDANCE TO LAWYERS ON HOW TO NAVIGATE CHANGING DATA FLOW LAWS

As the role of data continues to advance, in the United States, the new Biden Administration has stated that it would make cybersecurity and other data related issues "a top priority."[167] Nevertheless, it remains unclear whether the Biden Administration will pursue policies that favor local data storage requirements

---

164. Ridwan Oloyede, *Opportunities for Lawyers in Privacy and Data Protection,* LEGAL BUS. WORLD (Oct 17, 2019), https://www.legalbusinessworld.com/post/2019/10/17/opportunities-for-lawyers-in-privacy-and-data-protection [https://perma.cc/9VNX-6VGB].

165. MODEL RULES OF PROF'L CONDUCT R. 2.1 (2018) [hereinafter MODEL RULES].

166. MODEL RULES R. 2.1.

167. Emma Kinery, *Biden Calls Cybersecurity a 'Top Priority' After Russian Hack,* BLOOMBERG (Dec. 17, 2020), https://www.bloomberg.com/news/articles/2020-12-17/biden-calls-cybersecurity-a-top-priority-after-russian-hack [https://perma.cc/H9SL-LFMK].

similar to that of the Trump Administration.[168] If the new administration chooses to implement similar data localization requirements, the United States may face new risks to data security associated with data localization.[169] As mentioned in Section II, in the long-run, requiring data to be stored in one place or a few concentrated places may make the U.S. more vulnerable to data breaches and cybersecurity attacks because doing so eases the logistical burdens for hackers to collect information.[170]

The increased threat of cyber-attacks that could result should the U.S. continue to pursue data localization policies will likely affect many industries, including the legal field. Law firms are particularly attractive to hackers and therefore may be especially vulnerable to the consequences that result from cross-border data flow policies.[171] This attractiveness is largely because hackers often view law firms as easy targets that have "fewer security resources than their clients, with less understanding of and appreciation for cyber risk. As a result, hackers perceive law firms as potential "backdoors or gates" into their clients' valuable information.[172]

The advent of data security risks challenges lawyers' ability to carry out their duties of competence and confidentiality. First, attorneys have a longstanding duty to perform with adequate competency when representing clients.[173] ABA Model Rule 1.1 requires attorneys to have "legal knowledge. . . reasonably necessary for the representation."[174] In 2012, the ABA amended a comment to Rule 1.1 making it explicit that lawyers should "keep abreast of the changes in the law and its practice, *including the benefits and risks associated with relevant technology*.[175] As a result, practically speaking, the amended language may obligate lawyers to play a role in promoting effective data security both for their own law practices and for their clients' practices.[176] Threats to data security also necessarily implicate a lawyer's duties of confidentiality. Under Rule 1.6, lawyers "shall not reveal information relating to the representation of a client unless the client

168. For one account of the Trump Administration's policies, see Sam DuPont, *On TikTok, the Trump Administration is Adopting China's Own Vision for the Internet,* NEXTGOV (Sept. 22, 2020), https://www.nextgov.com/ideas/2020/09/tiktok-trump-administration-adopting-chinas-own-vision-internet/168667/ [https://perma.cc/H7QA-9R5V] ("In waging its digital trade war with China, the Trump administration has embraced China's own vision of data sovereignty: an internet that is walled off along national borders, blocking the free flow of data.").

169. Heidi F. Kuehl, *Technologically Competent: Ethical Practice for 21st Century Lawyering*, 10 CASE W. RES. J.L. TECH. & THE INTERNET 1, 5 (2019).

170. Chander & Lê, *supra* note 6, at 717.

171. Drew T. Simshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data*, 38 AM. J. TRIAL ADVOC., 549, 550 (2015).

172. *Id*. at 550–51.

173. Kuehl, *supra* note 169, at 5.

174. MODEL RULES R. 1.1.

175. MODEL RULES R. 1.1 cmt. 8 (emphasis added).

176. Simshaw, *supra* note 171, at 556.

gives informed consent."[177] The rule not only compels lawyers from refraining from revealing information but also provides that lawyers have the positive obligation to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[178] As the *ABA Cybersecurity Handbook* notes, the obligation to maintain confidentiality of client's representation "is no less applicable to electronically stored information than to information contained in paper documents, or not reduced to any written or stored form."[179] Rule 1.1 and 1.6 establish an "undeniable obligation for all attorneys to take affirmative steps to protect client information while practicing law" in the age of data security threats.[180]

The ethics rules present an opportunity for the broader legal community to help improve lawyers' data security practices to help them fulfill their ethical obligations and to mitigate cybersecurity risks that can result from changing cross-border data flow policies in the U.S. In order to do this, the broader legal community an provide guidance to lawyers on how to increase data security and to better navigate changing data flow laws.

First, the broader legal community—namely the American Bar Association or other state ethics bodies—can provide training and Continuing Legal Education (CLE) programs on proper data security compliance to ensure that lawyers are mitigating potential data security risks and meeting their ethical requirements. Bar-sponsored trainings and CLEs "can go a long way toward educating lawyers, who will then be better fit not only to ethically practice, but also to train other employees."[181]

In addition to providing training, given how fast technology develops, to stay up to date, the ABA can engage in research and analysis exploring how changes in cross-border data flow laws (both domestic and international) will affect and present challenges to the legal industry and other industries as well. The ABA can subsequently publish and distribute its findings to its members and other lawyers. The publication, similar to previous ABA publications such as *The Cybersecurity Handbook,*[182] could provide practical information about cross-border data flow laws, guidance, and even potential strategies that lawyers can use to navigate the issues that arise. At the same time, such a publication could spark conversation within the legal community as to how to further address the issues that arise because of quickly changing data flow laws.

---

177. MODEL RULES R. 1.6 (a).

178. MODEL RULES R. 1.6(a).

179. AM. BAR ASSOC., ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 62 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

180. Simshaw, *supra* note 171, at 565.

181. *Id.* at 571.

182. *See generally* JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: 3 A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS (2013).

Next, the ABA can create a special committee designed to address issues related to cross-border data flows, much like what the state of Georgia has done to address issues related to globalization.[183] The State Bar of Georgia, recognizing that the world was becoming increasingly globalized, created a supervisory committee called "The Committee on International Trade in Legal Services" to proactively address the challenges of globalization, cross-border legal practice, lawyer mobility, and bilateral and multilateral trade agreements affecting the regulation of legal services.[184] Similarly, a supervisory committee within the ABA could be created specifically to address data issues. This committee could have several functionalities. First, it can operate as a due diligence group that helps identify issues that lawyers now face as a result of changing data laws both within the United States and outside. That way, regulators may be able to consider these issues proactively rather than reactively. Additionally, the committee could collect information on approaches that have been used elsewhere in the world, including data about successes and failures. Third, the committee could look out for potentially developing new regulations abroad that would have a direct impact on U.S. lawyers and disseminate this information. Overall, a committee formed to specifically address data issues may allow for the legal community to not only better understand the legal and ethical issues that arise from these changes, but also respond swiftly and effectively.

CONCLUSION

We are seeing data localization phenomena with increasing frequency. Countries are starting to create laws that would require data to stay within its borders. This, in turn, has huge potential costs to international trade and the global economy. Current international regulatory regimes may not be able to adequately roll back excessive data localization measures. The novel issues and the technical complexity of data will likely require a range of new and creative solutions must be employed to more successfully govern data flows. The new issues that data localization present will likely require solutions on both the international front and domestic front.

183. *See generally* ABA Task Force on Int'l Trade in Legal Services, International Trade in Legal Services and Professional Regulation: A Framework for State Bars Based on the Georgia Experience (Feb. 4, 2012)

184. *Id.* at 10.