A SURVEY OF CROSS-BORDER DATA TRANSFER REGULATIONS THROUGH THE LENS OF THE INTERNATIONAL TRADE LAW REGIME

LINXIN DAI*

I. INTRODUCTION

The free movement of data across borders "underpins a growing range of economic activity and international trade."[1] Data flows have created new opportunities for businesses and spurred new sectors in the economy. The immense potential of data allows for "more efficient business operations, highly innovative societal solutions, and ultimately better policy choices."[2] Cross-border data flows provide multiple benefits for businesses, helping them to "access markets, interact with

* LL.M, New York University School of Law; LL.M candidate in International Economic Law and LL.B, China University of Political Science and Law. I would like to thank Ashley Miller, Andy Pigott, and their colleagues for their comments on an earlier draft of this article. All remaining errors are my own.

1. Aaditya Mattoo & Joshua P. Meltze, *International Data Flows and Privacy: The Conflict and Its Resolution* 3 (World Bank Group, Policy Research Working Paper No. 8431, 2018).

2. Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C. DAVIS L. REV. 65, 67 (2017).

customers across the globe, find new suppliers, and communicate with their overseas affiliates."[3]

Cross-border data flows lead to "higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security."[4] The non-rivalrous nature of data differentiates it from other resources and makes its transfer both much easier and much more difficult to control. These unique attributes present a challenge to the existing rules of the market and require regulators to adopt new approaches. These concerns may prompt national legislators to restrict data transfers across borders. Differing national approaches will lead to a wide range of measures adopted around the world.

Despite the possible benefits brought by the free flow of data transfers, recent decades have witnessed a tendency of countries to impose stricter regulations to restrict the free flow of data. This comment will discuss the national cross-border data transfer regulations that will impact international trade and the current cooperation regime countries have developed to overcome international trade law barriers.

II. Cross-Border Data Transfer Regulations

A. *Data Standards and Classifications*

Most regulations impose different levels of restrictions on personal and non-personal data. Some countries go further and adopt different data classifications to determine baseline security controls necessary for protection. However, the standard and classification of data may vary across jurisdictions, resulting in inconsistency in application and understanding.

Firstly, the boundaries between personal and non-personal data have become blurred. It is now possible to obtain personal data through the processing or analysis of non-personal data. Big data analytics is capable of examining massive amounts of diverse data to uncover hidden patterns and corre-

---

3. U.S. Dep't of Commerce, Measuring the Value of Cross-Border Data Flows iii (2016).

4. The Group of the Twenty (G20), *G20 Osaka Leader's Declaration*, ¶ 11 (June 29, 2019), https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf [hereinafter G20 Declaration].

lations.[5] This has raised concerns over privacy issues, as "the sheer scale and value of the data sets involved means they be a target for security breaches."[6]

Even within the area of personal data, there are various inconsistencies in global regulations. Most regulations define personal data as that which refers to information relating to "an identified or identifiable natural person."[7] However, some countries adopt a different standard. For example, the Australian Privacy Act provides that personal information includes any data about "an identified individual, or an individual who is reasonably identifiable."[8] Under the standard adopted by most international organizations, the main issues are when the subject of personal data can be said to be identifiable and what indirect identification means. For instance, the interpretation offered by the European Court of Justice is broad enough to include IP addresses.[9] On the other hand, the Italian Supreme Court concluded that, in some circumstances, the name and surname of an individual are not sufficient to identify the data subject.[10]

Other data classifications may pose additional challenges in determining the proper level of protection for certain data.

---

5. U.N. Conf. on Trade & Dev., Data Protection Regulations and International Data Flows: Implications for Trade and Development, 12, UNCTAD/WEB/DTL/STICT/2016/1/iPub (Apr. 2016).

6. *Id.*

7. Council Regulation 2016/679 of Apr. 27, 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, 33, art. 4(1) [hereinafter GDPR].

8. *Privacy Act 1988* (Cth) s 6 (Austl.) ("Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.")

9. *See* Case C-582/14, Breyer v. Germany, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri¢£LEX:62014CJ0582 (Oct. 19, 2016) (holding that "a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data.").

10. Massimiliano Pappalardo, *Personal Data or Non-personal Data, that is the Question! The Different Interpretations of ECJ and Italian Supreme* Court, LEXOLOGY (Oct. 25, 2016) https://www.lexology.com/library/detail.aspx?g=804ce9b8-dfa5-4c67-bbf7-4cc3e087c2f8.

For instance, China's Cybersecurity Law uses "important data" in addition to the term "personal information."[11] "Personal information" is defined as any information, "recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity."[12] The Law suggests that "important data" could include data closely related to national security, economic development, and social and public interests.[13] Further complicating the issue, the draft guidelines on determination of scope of cross-border data transfer under Chinese cybersecurity law gives the relevant government department discretion to further determine and analyze data on a case-by-case basis.[14]

B. *Data Localization*

Data localization refers to the restrictions on processing, transferring, and storing data in a jurisdiction other than where the data is generated.[15] Data localization is closely linked to national sovereignty concerns and has been used by many countries as a means to enhance national security, protect personal privacy, and support law enforcement.[16]

---

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

12. *Id.*

13. *See id.* (listing the purposes of the Law as to "ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society.").

14. *See* Qiheng Chen et al., *Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China*, NEW AM. (June 13, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/ ("After receiving the declaration material for personal information outbound transfer and verifying its completeness, province-level cybersecurity and informatization departments shall organize experts or technical capabilities to conduct security assessment.").

15. *Data Localization*, TECHNOPEDIA (May 8, 2017), https://www.techopedia.com/definition/32506/data-localization.

16. *See, e.g.*, Regulation No. 82 of 2012, Concerning Electronic System and Transaction Operation, art. 17(2) (Oct. 15, 2012) (Indon.) ("Electronic System Operator for the public service is obligated to put the data center

By restricting where and when data can be transferred and stored, data localization poses a barrier to the free flow of data across borders. Such requirements will impact the global economy and particularly the digital economy, which is driven by the ability to collect and use digital data,[17] including e-commerce, in the course of international trade. This economic impact would be magnified by the increased role of the internet in driving economic growth and determining global supply chains. Furthermore, a company under such data localization requirements may incur extra cost to host a data server in the jurisdictions where it collects and stores data. In fact, the economic loss caused by E.U. data localization measures could lead to a loss of output of fifty-two billion euros per year, representing 0.37% of E.U. GDP.[18]

There are a growing number of countries enacting and enforcing data localization laws to impose a ban on the transfer of personal data. For instance, Russia,[19] Indonesia,[20] and Vietnam[21] have required personal data to be stored on data servers or centers located within their jurisdiction. In China, the government has progressed from a fragmented legal framework requiring data localization for data in certain sectors, including health information,[22] credit information,[23] and

---

and disaster recovery center in Indonesian territory for the purpose of law enforcement, protection, and enforcement of national sovereignty to the data of its citizens.") [hereinafter Indonesia Regulation].

17. UNCTAD, Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries, at xv, UNCTAD/DER/2019, U.N. Sales No. E.19.II.D.17 (2019).

18. Matthias Bauer et al., *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States*, 2016 EUR. CTR. FOR INT'L POL. ECON. 1.

19. Federal Law of the Russian Federation on Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks, art. 2, 2014, No. 242-FZ.

20. Indonesia Regulation, *supra* note 16, art 17(2).

21. Law 24 on Cybersecurity, art. 26(3), National Assembly of the Socialist Republic of Vietnam, No. 2018/QH14 (June 12, 2018).

22. *Interpretation on Population Health Information Management Measures (Trial Implementation)*, NAT'L HEALTH & FAM. PLAN. COMM'N OF PRC (June 15, 2014) ("Organizations at all levels shall not store population health information on servers abroad, or on leased servers.").

23. U.S.-CHINA BUS. COUNCIL, TECHNOLOGY SECURITY AND IT IN CHINA: BENCHMARKING AND BEST PRACTICES 22 (2016), https://www.uschina.org/

online publishing,[24] to a uniform cybersecurity legal regime requiring data localization for all general personal data.[25] Some countries, such as Australia,[26] New Zealand,[27] and Turkey,[28] only restrict the transfer of data in specific sensitive sectors such as health information, tax records, and financing information. While these countries limit the application of data localization to certain sectors, the regulations continue to have a significant effect on global businesses. For example, in 2016 the data localization requirements in Turkey led to the suspension of PayPal's business after the company failed to comply with the regulation.[29]

---

sites/default/files/Technology%20Security%20and%20IT%20in%20China%20-%20%20Benchmarking%20and%20Best%20Practices.pdf ("Article 9.9 states that credit information service agencies operating in China must store all data collected in China within the country; sorting, storage, and processing must be done within China.").

24. Wangluò chuban fúwù guanli guiding (网络出版服务管理规定) [Provisions on the Administration of Online Publishing Services] (promulgated by the St. Admin. of Press, Publ'n, Radio, Film & Television (SARFT) and the Ministry of Indus., Admin., & Tech. Aug. 20, 2015, effective Mar. 10, 2016), art. 8(3) (China) (Online publishing services must keep all relevant storage devices and servers "within the territory of the People's Republic of China.")

25. Creemers, Triolo, & Webster, *supra* note 11, art. 37 ("Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China.").

26. *Personally Controlled Electronic Health Records Act 2012* (Cth) s 77 (Austl.) (specifying that holders of personally controlled electronic health records must not "hold the records, or take the records, outside Australia; or process or handle the information relating to the records outside Australia.").

27. Goods and Services Tax Act 1985, s 75(3BA) (N.Z.) (requiring goods and services records to be kept in New Zealand, or, with permission of the Commissioner, outside New Zealand).

28. Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, No. 6483, art. 23(1) (as amended by Law No. 6637 of Mar. 27, 2015) (June 20, 2013) (Turk.). ("The system operators shall be required to keep information systems and their substitutes which are used to carry out its activities in the country.").

29. Ingrid Lunden, *PayPal to Halt Operations in Turkey After Losing License, Impacts 'Hundreds of Thousands'*, TECHCRUNCH (May 31, 2016), https://techcrunch.com/2016/05/31/paypal-to-halt-operations-in-turkey-after-losing-license-impacts-hundreds-of-thousands/.

C. *Adequacy Requirements*

An adequacy requirement refers to the requirement that recipients of the data outside the sending country have adequate data protection measures. Adequacy requirements generally apply to the transfer of personal data and are imposed because of privacy concerns.

Adequacy requirements have an exterritorial impact and impose burdens on data recipients in jurisdictions which do not have data protection or have lower levels of data protection. Therefore, companies in such jurisdictions that do business with companies in jurisdictions with adequacy requirements will incur significant costs. If no or low protection companies receive data from adequacy requirement companies, they will have to build a protection regime, set up binding company rules, and provide binding commitments to apply appropriate safeguards. Otherwise, the data transfer will be suspended and monetary fines for violation will be imposed.[30]

The General Data Protection Regulation (GDPR) of the European Union requires that any transfer of personal data take place only under limited conditions, one of which is that data may only be transferred to third countries with an "adequate level of protection" as determined by the European Commission.[31] In the absence of adequate protections in the receiving country, transfer of data is allowed only if the "appropriate safeguards" are provided.[32] In addition to the GDPR, countries including Singapore,[33] Thailand,[34] and Australia[35]

---

30. *See* Jon Levitt & Bill Stone, *Even if You Are a U.S. Company, Don't Ignore the GDPR*, OUTSIDE GC (May 4, 2018), https://www.outsidegc.com/blog/compliance-with-gdpr-eu-data-privacy-law ("The GDPR includes significantly increased penalties for violations, with fines as high as €10M or 2% of annual worldwide revenue, or €20M or 4% of annual worldwide revenue, depending on the type of violation.").

31. GDPR, *supra* note 7, at 61, art. 45(1).

32. *Id.* art. 46(1).

33. Personal Data Protection Act 2012, No. 26, Gov. Gazette Acts Supp. art. 26 (Sing.) ("An organization shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organizations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act." Exemptions to this requirement can be granted by the Personal Data Protection Commission.)

34. Personal Data Protection Act, B.E. 2562, sec. 28, Gov. Gazette No. 136 Chapter 69 Gor (May 27, 2019) (Thai.) ("In the event that the Data

provide similar requirements regulating cross-border data transfers, though processes differ from country to country.

III. Cross-Border Data Transfer Under the International Trade Law Regime

A. *World Trade Organization (WTO)*

The General Agreement on Trade in Services (GATS) covers four modes of supply for the delivery of services in cross-border trade, including cross-border supply and commercial presence.[36] To assess whether the data transfer regulations of a WTO member violate the GATS, the mode of the data transfer and the relevant service sector are determined first, and the commitment of the member for the sector is then assessed.[37]

Article VI of the GATS states that generally applicable measures affecting trade in services must be "administered in a reasonable, objective and impartial manner."[38] Furthermore, measures such as qualification requirements and procedures, technical standards, and licensing requirements must not create unnecessary barriers to trade in services or nullify member commitments.[39] It is argued that Article VI does not leave member states much discretion to introduce a high privacy standard, as "any cross-border restriction is at risk to be challenged."[40] Certain measures adopted by member countries,

---

Controller sends or transfers the Personal Data to a foreign country, the destination country or international organization that receives such Personal Data shall have adequate data protection standard," unless enumerated circumstances are met).

35. *Information Privacy Act 2014* (ACT) sch 1 pt 1.3 s 8(1) (Austl.) ("Before a public sector agency discloses personal information about an individual to a person (an *overseas recipient*) . . . the agency must take reasonable steps to ensure that the overseas recipient does not breach the TPPs (other than TPP 1) in relation to the information.").

36. General Agreement on Trade in Services art. I, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization Annex 1B, 1869 U.N.T.S. 183 [hereinafter "GATS"].

37. 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, 197 (2018).

38. GATS, *supra* note 40, art. VI(1).

39. *Id.* arts. VI(4)–(5).

40. Rolf H. Weber, *Regulatory Autonomy and the Privacy Standards Under the GATS*, 7 Asian J. WTO & Int'l Health L. & Pol'y 25, 37 (2012).

such as requiring authorization from a data protection commission, may increase the costs attendant on (and thus erect extra barriers to) cross-border data transfers.

When countries adopt high privacy standards and rules requiring the local processing of financial information, the national scheme may constitute a de facto limit, or even prohibition, on the access of foreign operators. Under Article XVI, member states may not undertake measures that impair market access, such as limiting the number of service suppliers and the total value of service transactions or assets.[41] In *China – Electronic Payment Services*, the WTO Panel found that China acted inconsistently with GATS art. XVI:2(a) because only China UnionPay was authorized to clear RMB-denominated transactions involving RMB payment cards.[42] In *US – Gambling*, the WTO Appellate Body affirmed the Panel's decision that the United States acted inconsistently with Art. XVI:1 and 2 by prohibiting the cross-border supply of gambling and betting services.[43]

B. *Free Trade Agreements*

Free trade agreements have become another means of regulating cross-border data transfers, especially in the sector of digital trade. The two relevant agreements are the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[44] and the United States-Mexico-Canada Agreement (USMCA).[45] Both agreements encourage and promote cross-border data transfer with the aim of improving of digital trade.

---

41. GATS, *supra* note 40, art. XVI(2).

42. Panel Report, *China—Certain Measures Affecting Electronic Payment Services*, WTO Doc. WT/DS413/R (adopted Aug. 31, 2012).

43. Appellate Body Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R/Corr.1 (adopted May 22, 2007).

44. Comprehensive and Progressive Agreement for Trans-Pacific Partnership, art. 14.11(2), Mar. 8, 2018, New Zealand Treaties Online, https://www.treaties.mfat.govt.nz/search/details/t/3911 [hereinafter CPTPP].

45. Agreement Between the United States of America, the United Mexican States, and Canada 12/13/19 Text, Office of U.S. Trade Representative, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between [hereinafter USMCA].

1. *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*

The CPTPP provides that parties shall "allow the cross-border transfer of information by electronic means."[46] Moreover, such information includes personal information if it is for the conduct of business.[47] This provision is contrary to the regulations examined above which require the flow of personal information to be restricted to protect privacy. Furthermore, Article 14.13 prohibits localization requirements calling for computing facilities within the jurisdiction as a condition for conducting business in that party's territory.[48] This provision directly opposes data localization requirements, but it does contain an exemption to the regulation for parties who have adopted such requirements into their national legal regimes, such as Vietnam.[49] Furthermore, because financial institutions and financial service providers are excluded from the scope of the article,[50] the prohibition on data localization does not apply to information they use, including personal financial information.

2. *United States-Mexico-Canada Agreement*

The USMCA includes similar arrangements regarding cross-border data flows and data localization. Compared to the CPTPP, the USMCA goes even further in avoiding barriers to the use and development of digital trade and data transfers. First, the USMCA uses the term digital trade instead of electronic commerce. Though the two terms are similar, the latter focuses on the flow of goods through the internet, while the former emphasizes the flow of digitalized content and services, focusing on data flows.[51] Second, the USMCA enlarges its scope to include "interactive computer services"[52] and "open government data,"[53] meaning the parties agree to promote in-

46. CPTPP, *supra* note 44, art. 14.11(2).
47. *Id.*
48. *Id.* art. 14.13(2).
49. *Id.* art. 14.13(3).
50. *Id.* art. 14.1.
51. Emily Benson, *E-Commerce vs. Digital Trade*, BERTELSMANN FOUND. (Dec. 20, 2019), https://www.bfna.org/research/e-commerce-vs-digital-trade/.
52. USMCA, *supra* note 45, art. 19.17.
53. *Id.* art. 19.18.

teractive computer services and facilitate public access and use of government information. Third, the USMCA incorporates and recognizes the guidelines of other international bodies, referencing APEC Cross-Border Privacy Rules and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.[54] These provisions enable parties to better adhere to both the requirements under the agreement and preexisting regimes.

C. *Further Development*

In January 2019, seventy-six partners of the WTO decided to start negotiations to establish global rules on electronic commerce, aiming to enhance opportunities, address the challenges of e-commerce, and ultimately create a multilateral legal framework.[55]

In June 2019, leaders of the G20 made a declaration concerning innovation of digitalization and secure free flows of data, stating that facilitating data free flow and strengthening consumer and business trust are essential to economic growth.[56] The G20 agreed that the free flow of data with trust "will harness the opportunities of the digital economy" and encouraged countries to cooperate to achieve interoperability among frameworks.[57]

IV. Conclusion

For the purpose of protecting privacy and national security, countries have enacted regulations restricting cross-border data transfer. However, the inconsistency of data standards and classifications, data localization requirements, and adequacy requirements across national regimes will impose compliance burdens and costs on companies engaged in digital trade. Furthermore, strict regulations may conflict with the existing legal obligations of international trade under the WTO regime. Some countries have tried to eliminate digital trade

54. *Id.* arts. 19.8, 19.14.

55. Press Release, European Commission, 76 WTO Partners Launch Talks on E-Commerce (Jan. 25, 2019), http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974.

56. G20 Declaration, *supra* note 4, ¶¶ 1, 10.

57. *Id.* ¶ 11.

barriers through FTAs. For instance, in the CPTPP and the USMCA, parties have agreed to promote the free flow of data and to prohibit the required localization of computing facilities. However, the conflicts between data protection in different jurisdictions and free international trade have not been solved. The current inconsistencies make the system unworkable and require a fresh approach that reconciles concerns regarding both data protection and free international trade.