The Emerging Model for Harmonizing Cross-Border Data Transfer Laws: From the APEC's to the Global CBPR Framework

Yueh-Ping (Alex) YANG*

Abstract

Cross-border data transfer is a controversial topic in modern digital trade law due to the different positions of major economies. While several efforts to harmonize cross-border data transfer laws have been made in the multilateral or regional forum, real progress remains limited. In this chapter, I focus on an emerging model for promoting cross-border data transfer, the Global Cross-Border Privacy Rules ("CBPR") Framework. I review and discuss CBPR's design and features, including the soft-law nature, the public-private gatekeeper model, and the bottom-up approach. I argue that CBPR introduces a novel approach for harmonizing cross-border data transfer with good rationales and deserves more scholarly attention.

Keywords: cross-border data transfer; GDPR; DEPA; APEC; CBPR; accountable agent

I. Introduction

The world is now in a war of cross-border data transfer. Across the Atlantic, the European Union ("EU") and the United States have debated the legality of data transfer from the former to the latter for a decade, featured by the series of *Schrems* cases.[1] Across the Pacific, China and the United States had apparent disagreements regarding how to deal with the data possessed by Chinese companies having overseas operations.[2] Even the United States, the major advocate of free cross-border data flow, seems to have second thoughts recently.[3] Foreseeably, the world will witness increasing restrictions on cross-border data transfer in the near future.

* Associate Professor, National Taiwan University Department of Law. Director, Asian Center for WTO & International Health Law and Policy of National Taiwan University College of Law. Co-Chair, WTO Chair Programme (Phase III). The author is grateful for the research assistance provided by Julian Luo, Yun-Wei Chen, Hao-Wen Zheng, and Fu-Tai Yen. The author can be reached at alexypyang@ntu.edu.tw.
The research is sponsored by WTO's WTO Chair Programme (Phase III).

[1] Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015); Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd, ECLI:EU:C:2020:559 (July 16, 2020).

[2] The representative dispute that sparked the China-US disagreement was the Didi dispute in 2021, a significant event that provides a real-world context for cross-border data transfer issues. For an introduction, *see* Elizabeth Zhou, *Cross-Border Transfer of Data: Case Study of Didi* (July 9, 2021), https://blogs.ischool.berkeley.edu/w231/2021/07/09/cross-border-transfer-of-data-case-study-of-didi/.

[3] *See infra* II.A.c.

International economic laws have recognized the pressing issue of cross-border data transfer and tried to harmonize the laws across different jurisdictions.[4] These efforts are mainly seen in several regional trade agreements, e.g., the United States United States-Mexico-Canada Agreement ("USMCA"), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP"), the Digital Economy Partnership Agreement ("DEPA"), and Regional Comprehensive Economic Partnership ("RCEP"). However, these efforts have remained mainly in abstract ideas and concepts. As the United States starts to have second thoughts on promoting free cross-border data flow, the future of these harmonization efforts appears dim.

In this chapter, I highlight an evolving yet less-noticed[5] model for facilitating cross-border data transfer: the Global Cross-Border Privacy Rules (CBPR) Framework,[6] which is expanded from the CBPR System under the Asia-Pacific Economic Cooperation (APEC).[7] Unlike the approach adopted in regional trade agreements such as USMCA, CPTPP, DEPA, or RCEP, the Global CBPR Framework takes a unique approach. It introduces a public-private-partnership gatekeeper model and a soft-law approach to establish standards for facilitating cross-border data transfer. While its success in practice remains to be observed, it deserves more attention from a theoretical perspective.

This chapter is structured as follows. Section II briefs the divergent cross-border data transfer laws across different jurisdictions. Section III describes the attempts made in several regional trade agreements to promote cross-border data transfer. Section IV introduces the Global CBPR Framework, featured by its unique Accountability Agent ("AA") design. Section V reflects on the Global CBPR Framework by elaborating on its theoretical advantages, discussing the critics, and identifying its future challenges. Section VI concludes this chapter. While the world has acknowledged the importance of harmonizing cross-border data transfer laws, it is anticipated that this chapter may inject different perspectives on "how" to facilitate the harmonization.

II. The Current Landscape of Cross-Border Data Transfer Laws Around the World

[4] For related literature, *see, e.g.,* Andrew D. Mitchell & Neha Mishra, *Cross-Border Data Regulatory Frameworks: Opportunities, Challenges, and a Future- Forward Agenda*, 34 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 842 (2024); Douglas W. Arner et al., *The Transnational Data Governance Problem*, 37 BERKELEY TECH. L.J. 623 (2022); Anupam Chander & Haochen Sun, *Sovereignty 2.0*, 55 VAND. J. TRANSNAT'L L. 283 (2022); Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017).

[5] For CBPR-related studies, *see, e.g.,* Shin-Yi Peng, *Public–Private Interactions in Privacy Governance*, 11(6) LAWS, MDPI 80 (2022); Anupam Chander & Paul Schwartz, *Policy and/or Trade*, 90(1) U. CHI. L. REV. 49, 95-98 (2023).

[6] Global CBPR Forum, https://www.globalcbpr.org/ (last visited Aug. 11, 2024).

[7] Cross Border Privacy Rules System, https://cbprs.org/ (last visited Aug. 11, 2024).

Many commentators have observed that nowadays, the world's cross-border data transfer laws feature the "Three Digital Kingdoms" landscape.[8] EU, China, and the United States perceive cross-border data transfer differently, imposing different restrictions.

A. European Union

As many commentators have observed, the EU's stance on cross-border data transfer features a privacy-oriented model. Its general regulation of cross-border data transfer is laid down in the General Data Protection Regulation ("GDPR"), which protects the fundamental rights and freedoms of natural persons, particularly their personal data rights.[9] GDPR's Chapter 5 further regulates cross-border data transfer to ensure that its level of personal data protection is not undermined.[10]

Under this regime, cross-border data transfer is prohibited unless in exceptional circumstances. These exceptions, in general, include:

i. Based on an adequacy decision, i.e., where the European Commission has decided that the third country receiving the data transfer ensures an adequate level of protection;[11]

ii. Based on the appropriate safeguards adopted by the data processor or controller.[12] GDPR further enumerates these safeguards as:[13]

- Legally binding and enforceable instrument between public authorities or bodies;
- Binding corporate rules;
- Standard contractual clauses;
- Approved codes of conduct;
- Approved certification mechanism.

iii. Based on other exceptions, i.e.,

[8] *See generally* Henry S. Gao. *Data Sovereignty and Trade Agreements: Three Digital Kingdoms, in* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 213 (Anupam Chander & Sun Haochen eds., 2024).
[9] GDPR, art. 1.2 (EU).
[10] GDPR, art. 44(2) (EU).
[11] GDPR, art. 45.1(1) (EU).
[12] GDPR, art. 46.1 (EU).
[13] GDPR, art. 46.2 (EU).

- Explicit consent by the data subject;[14]
- Other necessary measures;[15]
- Made by a register intended to provide information to the public and open to consultation;[16]
- Necessary for compelling legitimate interests pursued by the controller.[17]

Based on the above cross-border data transfer regulations, the EU may examine not only the appropriateness of the safeguards adopted by data controllers or processors but also the adequacy of other countries' personal data protection laws. Through these regulations, the data protection level adopted in the GDPR *de facto* governs other countries. This unilateral implementation of the data protection level in other countries, thus, leads to the concern of GDPR's "Brussels Effect"[18] and the potential WTO inconsistency.[19]

On the other hand, it is noteworthy that GDPR ensures unrestricted data flow within the EU[20] based on the presumption that EU member states are GDPR-compliant and maintain a high level of personal data protection. Therefore, GDPR effectively restricts data outflow to non-EU countries while facilitating the data flow within EU member states. This result somehow fits the EU's industrial interests, which is more of a data exporter and thus needs more restrictions on the data outflow to protect its data industry and sovereignty.[21]

B. China

China's stance on cross-border data transfer is similarly less keen on free data flow, particularly free data outflow. However, China's rationale differs because it restricts cross-border data transfer for not only personal data protection but also national security reasons.

---

[14] GDPR, art. 49.1(1)(a) (EU).
[15] GDPR, art. 49.1(1)(b)~(f) (EU).
[16] GDPR, art. 49.1(1)(g) and 49.2 (EU).
[17] GDPR, art. 49.1(2) (EU).
[18] ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 131-70 (2019).
[19] *See, e.g.,* Tsai-Fang Chen, *Non-Discrimination Under the Most-Favoured-Nation Obligation and Adequacy Decisions in the General Data Protection Regulation*, 18(2) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 309 (2023). *See also* Elisabeth Meddin, *The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services*, 35(4) AM. U. INT'L L. REV. 997 (2020).
[20] GDPR, art. 1.3 (EU).
[21] *See* Chander & Sun, *supra* note 5, at 298-99.

Regarding personal data protection, according to China's Personal Information Protection Law ("PIPL"), data processors must obtain the data subject's informed consent before transferring the personal information out of China.[22] Besides the informed consent, they must satisfy any of the following conditions:[23]

- Undergoing the security assessment of the national cyberspace information authorities;[24]
- Obtaining the personal information protection certification conducted by professional institutions;
- Concluding an agreement with the foreign data receiver in accordance with the standard contractual clauses;
- Others stipulated by laws, regulations, or national cyberspace information authorities.[25]

In other words, unlike the GDPR, which allows data controllers to conduct cross-border data transfer based on the adequacy decision or appropriate safeguards without data subjects' consent, China requires data subjects' consent as a prerequisite and imposes additional requirements on top of it. Therefore, China effectively maintains more restrictive cross-border data transfer laws than the EU, even in terms of personal data protection.

Moreover, China's cross-border data transfer laws feature its concern over cyberspace security. China's Data Security Law ("DSL"), promulgated in 2021, introduced a data outflow security management regime to regulate the data outflow conducted by critical information infrastructure operators and other critical data outflow made by general data processors.[26] Specifically, these data outflow activities may not be performed unless approved by the data outflow security assessment conducted by the national cyberspace information authorities.[27] Notably, the data subject to the said regulation refers to any records of information by electronic or other

---

[22] PERSONAL INFORMATION PROTECTION LAW (个人信息保护法), art. 39 (China).
[23] PERSONAL INFORMATION PROTECTION LAW, art. 38.1 (China).
[24] Specifically, critical information infrastructure operators and data processors that process personal information that reaches the amount stipulated by the national cyberspace information authorities must store the collected and produced personal information domestically unless permitted by the security assessment conducted by the national cyberspace information authorities. PERSONAL INFORMATION PROTECTION LAW, art. 40 (China).
[25] China recently promulgated the Regulation for Facilitating and Regulating Cross-Border Data Flow in 2024, which introduced several exceptions to the cross-border data transfer regulation. *See* REGULATION FOR FACILITATING AND REGULATING CROSS-BORDER DATA FLOW (促进和规范数据跨境流动规定), art. 5 (China).
[26] DATA SECURITY LAW (数据安全法), art. 31 (China).
[27] DATA OUTFLOW SECURITY ASSESSMENT REGULATION (数据出境安全评估办法), art. 4 (China).

means,[28] which include personal and non-personal information.

Based on the PIPL and DSL, any data processors that transfer critical data,[29] the personal information of 100 million people or more, or the sensitive personal information[30] of 10 million people abroad shall file for data security assessment.[31] The security assessment regime inevitably introduces more state intervention in cross-border data transfer in China. This security-oriented attitude toward cross-border data transfer also fits China's political ideology, prioritizing national security and state control.

C. United States

In contrast to the previous two countries, the United States holds a more liberal view on cross-border data transfer. The United States has neither adopted general data or personal information protection laws in place nor designated a federal agency in charge of data regulations. Related data or privacy regulations in the United States, if any, are scattered in various sectors or state laws, resulting in the absence of cross-border data transfer laws in the United States. This liberal attitude toward free data flow also fits the advantages of the United States in the data industry, which is the major data-importing country in the world.[32]

However, the United States seems to have taken a step back recently. In October 2023, the United States, as the major advocate of free cross-border data transfer in WTO's E-Commerce negotiations, removed its support for the said negotiations.[33] In February 2024, President Biden issued an executive order that required the U.S. Department of Justice to issue regulations that establish clear protections for Americans' sensitive personal data, such as genomic data, biometric data, personal health data, geolocation data, financial data, from access and exploitation by countries of concern.[34]

---

[28] DATA SECURITY LAW, art. 3.1 (China).

[29] Critical data refers to the data that, once altered, damaged, leaked, or being acquired or used illegally, might endanger the national security, economic operation, social stability, public health and safety, etc. DATA OUTFLOW SECURITY ASSESSMENT REGULATION, art. 19 (China).

[30] Sensitive personal information refers to the personal information that, once leaked or used illegally, may easily result in the infringement of the human dignity or damage to the personal or property security of natural persons, including biometrics, religion, specific identity, medical health, financial accounts, trail records, etc. and personal information of minors younger than 14 years old. PERSONAL INFORMATION PROTECTION LAW, art. 28 (China).

[31] DATA OUTFLOW SECURITY ASSESSMENT REGULATION, art. 4 (China).

[32] *See* Chander & Sun, *supra* note 5, at 301-02.

[33] Office of the United States Trade Representative, USTR Statement on WTO E-Commerce Negotiations (Oct. 24, 2023), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations

[34] The White House, Fact Sheet: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data (Feb. 28, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

This recent change might introduce the first cross-border data transfer regime in the United States in the foreseeable future.[35]

The recent change of attitude of the United States coincides with the industrial relations between the United States and other countries, particularly China. Due to China's cyber control, the United States' internet giants, such as Amazon, Google, and Facebook, have limited, if any, access to China's market. In contrast, China's internet giants are free to operate in the United States, while some, such as TikTok and SHEIN, have reached tremendous success. This imbalance undeniably places the United States at a disadvantageous industrial position, which might explain the United States' shift of attitude against free cross-border data flow.

D. Summary

In sum, different jurisdictions perceive cross-border data transfer differently due to their difference in industrial structure, consumer protection commitment, privacy protection level, national policy, etc. These vast gaps render it challenging to coordinate a solution at a state-to-state level, which will be discussed in the next Section.

III. The Current Attempts to Address the Divergence

Different cross-border data transfer laws inevitably conflict. Therefore, different methods are developed to address this conflict. In this Section, I will discuss two prominent examples: the unilateral approach, which is the default rule, and the bilateral approach adopted in some regional trade agreements.

A. The Unilateral Approach

The default rule for addressing the conflict of cross-border data transfer laws is that each country may impose its data laws on other countries unilaterally. After all, each country possesses the sovereignty to regulate data controllers within its jurisdiction. Domestic data controllers inevitably need to abide by their countries' cross-border data transfer laws to transfer data abroad.

The apparent impact of this unilateral approach is that each country's data laws will apply cumulatively to cross-border data controllers and, thus, increase their compliance costs. The compliance costs will be multiplied for multinational data controllers conducting data-related businesses in multiple jurisdictions. In some jurisdictions that maintain more restrictive cross-border data transfer laws, these data controllers may even find it prohibitive to transfer the data. In sum, cross-border data

[35] Luke Schaetzel, *United States Looks Towards its First Cross-Border Data Transfer Regime with New Executive Order*, BENESCH (Mar. 24, 2024), https://www.beneschlaw.com/resources/united-states-looks-towards-its-first-cross-border-data-transfer-regime-with-new-executive-order.html.

transfer will be costly and restrictive, resulting in a less efficient deployment of resources for storing, transferring, and processing data on a global scale.

Recognizing this potential dilemma, some jurisdictions attempt to facilitate cross-border data transfer by adopting the unilateral approach. For instance, the EU adopted the adequacy decision regime to balance cross-border data transfer and privacy protection. In a nutshell, it assesses the adequacy of a country's overall personal data protection level, including its rule of laws, respect for human rights and fundamental freedoms, relevant legislation, the implementation of such legislation, the existence and effective functioning of one or more independent supervisory authorities, and the international commitments, etc.[36] Transferring data to the countries determined by the EU as adequate needs not abide by other GDPR rules on cross-border data transfer. As of July 2024, the EU has recognized 15 countries as providing adequate protection.[37]

However, the adequacy decision regime, in essence, remains unilateral. After all, the EU is the authority that determines the adequacy of each country, and its decision may be arbitrary.[38] In practice, the EU actively conducts adequacy decisions, even against the United States. The famous *Shrems* disputes between the EU and the United States exhibit that the EU rigorously reviewed the United States' personal data protection laws, including national intelligence laws. Moreover, after finding inadequate protection of the personal data rights of its citizens, the EU, or at least the Court of Justice of the European Union, did not hesitate to cancel the adequacy decision. Therefore, the EU's adequacy decision regime is not a free lunch for data-receiving countries.

If most jurisdictions adopt this unilateral approach and "export" their data laws to others, the worst scenario is that multinational data controllers cannot conduct cross-border data transfer and shall instead store and process the data locally. This will inevitably create severe storage and processing costs for these companies, which is not necessarily an efficient outcome.

B. The Bilateral Approach

Given the apparent shortcomings of the unilateral approach, many jurisdictions have started to coordinate their cross-border data transfer laws bilaterally. Some

---

[36] GDPR, art. 45.2 (EU).

[37] These countries include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom, the United States, and Uruguay. European Commission, *Adequacy Decisions*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Aug. 11, 2024).

[38] Some literature criticizes the EU's arbitrary selection of priority countries for its adequacy decision. *See* Meddin, *supra* note 19, at 1016-18.

progress has been made in several regional trade agreements. Below, I introduce four of them: the USMCA, CPTPP, DEPA, and RCEP.

a. USMCA

Led by the United States, the USMCA introduces several provisions on cross-border data transfer, which reflects the United States' stance on free data flow.

First, the USMCA stipulates the principle that the cross-border data transfer between Parties should not be restricted while permitting a wide range of exceptions. Its Article 19.11(1) provides that "[n]o Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person."

However, Article 19.11(2) immediately follows that,

> This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is *necessary to achieve a legitimate public policy objective*, provided that the measure:
>
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
>
> (b) does not impose restrictions on transfers of information *greater than are necessary* to achieve the objective.

In essence, the cross-border data transfer clause under the USMCA adopts a "necessity" test, coupled with the familiar "arbitrary discrimination" test, as the exception for a Party to limit cross-border data transfer between Parties. Notably, any "legitimate public policy objective" may serve as grounds for justifying the restriction to cross-border data transfer, which exhibits the flexibility of this exception compared with GATT Art. XX or GATS Art. XIV. That said, a Party still needs to pass the necessity test to restrict cross-border data transfer between Parties, which inevitably limits its room to adopt said restrictions.

On the other hand, while facilitating cross-border data transfer through the above clause, the USMCA does not ignore the potential privacy concern associated with said transfer. Article 19.8(2) requires each Party to "*adopt or maintain a legal framework* that provides for the protection of the personal information of the users of digital trade." Moreover, to ensure that each Party adopts an adequate privacy protection framework, it encourages each Party to "take into account *principles and guidelines of relevant international bodies*, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of

Privacy and Transborder Flows of Personal Data (2013)." In sum, the USMCA addresses the privacy concern of cross-border data transfer by requiring Parties to establish a minimum privacy protection framework based on available international standards.

Finally, the USMCA encourages Parties to harmonize their privacy protection frameworks to address the potential conflict and mitigate the compliance cost of cross-border data processors. Article 19.8(6) prompts Parties to "encourage the development of mechanisms to promote compatibility between these different regimes" and requires Parties to "endeavor to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them." While these provisions are relatively soft and abstract, they notably identify the APEC's CBPR System as "a valid mechanism to facilitate cross-border information transfers while protecting personal information," which will be discussed more in Section IV.

b. CPTPP

CPTPP resembles the USMCA's efforts to promote cross-border data transfer while ensuring minimum privacy protection as the basis. Its Article 14.11(2) similarly requires each Party to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person," which sets the principle of free cross-border data transfer. On the other hand, Article 14.11(3) also stipulates the exception for restricting cross-border data transfer by providing that,

> Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
>
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
>
> (b) does not impose restrictions on transfers of information *greater than are required* to achieve the objective.

To be sure, CPTPP does not follow the USMCA in specifically limiting the exception to restrictions that are "necessary" to achieve a legitimate public policy objective. However, subparagraph (b) requires the restrictions not to be "greater than required," which bears the necessity elements. Therefore, one may understand CPTPP as adopting a softer version of the necessity test to govern parties' restrictions to cross-border data transfer.

On the other hand, CPTPP's Article 14.8(2) also requires Parties to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce" and encourage parties to "take into account principles and guidelines of relevant international bodies." However, slightly different from the USMCA, CPTPP does not explicitly indicate the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) as the relevant international bodies.

CPTPP also recognizes the importance of harmonizing the privacy protection frameworks between Parties and similarly prompts Parties to "encourage the development of mechanisms to promote compatibility between these different regimes" in its Article 14.8(5). However, unlike the USMCA, which identifies the APEC Cross-Border Privacy Rules system as a specific harmonization mechanism, Article 14.8(5) only enumerates several general mechanisms, such as "the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks."

In general, CPTPP resembles the USMCA's model. It similarly prohibits the restriction on cross-border data transfer as a principle while adopting a softer necessity test as the exception. It also requires Parties to adopt privacy protection frameworks based on international standards and encourages parties to harmonize their frameworks. It differs from the USMCA mainly in that it does not explicitly identify the APEC privacy framework and APEC's CBPR System.

c. DEPA

DEPA is widely perceived as a novel breakthrough in international digital laws. However, on cross-border data transfer, DEPA generally resembles CPTPP. Article 4.3(2) similarly requires each Party to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person," which stipulates free cross-border data transfer as the principle. Article 4.3(3) also similarly provides for a softer necessity test as the exception, providing that,

> Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
>
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information *greater than are required* to achieve the objective."

DEPA's Article 4.2(2) also resembles the USMCA and CPTPP in requiring each Party to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce and digital trade," tak[ing] into account principles and guidelines of relevant international bodies." Besides, like CPTPP, DEPA does not explicitly indicate that the APEC Privacy Framework and the OECD Recommendation are relevant international bodies.

DEPA differs from the USMCA and CPTPP in emphasizing mechanisms for harmonizing Parties' privacy protection frameworks. Like the USMCA and CPTPP, DEPA's Article 4.2(6) requires each Party to "pursue the development of mechanisms to promote compatibility and interoperability between their different regimes for protecting personal information." That said, it enumerates more harmonization mechanisms that have the potential to pave the way forward, including (a) the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement; (b) broader international frameworks; (c) where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or (d) other avenues of transfer of personal information between the Parties.

Among these harmonization mechanisms, DEPA particularly highlights the "national trustmark" in the following manner:

- Requiring Parties to "encourage adoption of data protection trustmarks by businesses that would help verify conformance to personal data protection standards and best practices;"[39]
- Requiring Parties to "exchange information on and share experiences on the use of data protection trustmarks;"[40]
- Requiring Parties to endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information.[41]

d. RCEP

RCEP is less aggressive in cross-border data transfer than in the previous three agreements. While RCEP's Article 12.15(2) similarly requires parties not to "prevent

[39] DEPA, art. 4.8.
[40] DEPA, art. 4.9.
[41] DEPA, art. 4.10.

cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person," Article 12.15(3) provides for a broader exception clause for this obligation, i.e.:

> Nothing in this Article shall prevent a Party from adopting or maintaining:
>
> (a) any measure inconsistent with paragraph 2 that *it considers necessary* to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or
>
> (b) any measure that *it considers necessary* for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

By using the phrase "it considers necessary," as opposed to the "necessary" or "greater than are required" under the USMCA, CPTPP, or DEPA, RCEP adopts a subjective rather than objective necessity test to permit restrictions on cross-border data transfer. RCEP also makes it clear that "the necessity behind the implementation of such legitimate public policy *shall be decided by the implementing Party*."[42] This exception clause expands the room for parties to justify their restrictions on cross-border data transfer.[43]

On the other hand, RCEP's Article 12.8(1) and (2) similarly require parties to "adopt or maintain a legal framework which ensures the protection of personal information of the users of electronic commerce," "tak[ing] into account international standards, principles, guidelines, and criteria of relevant international organisations or bodies." However, on how to harmonize the different frameworks between parties, RCEP's Article 12.8(5) merely requires parties to "cooperate, to the extent possible, for the protection of personal information transferred from a Party."

Overall, while RCEP similarly requires free cross-border data transfer as the principle, it permits a broader scope of exceptions for parties to restrict cross-border data transfer based on the subjective necessity test. It also mentions less about the mechanisms for harmonizing parties' personal information protection frameworks. In

---

[42] RCEP, Chap. 12, Fn 14.

[43] To be sure, this does not mean that parties may impose restrictions without any limits. For instance, in interpreting the same term "it considers necessary" under the security exception clause of GATT Art. XXI(b), although the Panel agreed that the implementing Member may determine the necessity of the measures for the protection of its essential security interests, the Panel found, based on the obligation of good faith, that the measures at issue must "meet a minimum requirement of plausibility in relation to the proffered essential security interests." That means the Panel may still review whether the measure is "so remote from, or unrelated to," the alleged essential security interests. Panel Report, Russia – Measures Concerning Traffic in Transit, WT/DS512/R, ¶¶ 7.138-7.139, 7.146 (Apr. 5, 2019). Therefore, the subjective necessity test adopted in RCEP might not be a purely self-judging exception. That said, it adopts a looser "plausibility test" than the objective necessity test under USMCA, CPTPP, or DEPA.

general, RCEP preserves broad discretion for parties to determine whether to restrict cross-border data transfer.

C. Summary

Despite various attempts to harmonize cross-border data transfer laws between jurisdictions, achievements at the state-to-state level appear little. In those cases that reach some bilateral consensus, such as the USMCA, CPTPP, or DEPA, their progress remains limited, if any. In most cases, they adopt relatively abstract terms prohibiting cross-border data transfer restrictions as the principle. However, they also provide ample room for exceptions based on abstract terms, such as legitimate public policy objectives, coupled with the conventional necessity and arbitrary discrimination tests. Therefore, this bilateral approach can hardly prevent certain countries, such as the EU or China, from restricting cross-border data transfer based on personal data or national security protection concerns.[44] Not to mention RCEP, which provides parties with even broader discretion.

Moreover, many countries still do not support the above bilateral approach. EU, for instance, is not a party to any of the USMCA, CPTPP, or DEPA, and its stance remains prioritizing personal data protection over cross-border data transfer. Therefore, the EU appears uncomfortable with the exception clauses in the above bilateral approach even though they have provided flexibility for restricting cross-border data transfer. In its proposals for the Joint Statement on Electronic Commerce, the EU makes it clear that "[m]embers may adopt and maintain the safeguards *they deem appropriate* to ensure the protection of personal data and privacy, *including through the adoption and application of rules for the cross-border transfer of personal data*" and further emphasized that "[n]othing in the agreed disciplines and commitments shall affect the protection of personal data and privacy afforded by the Members' respective safeguards."[45]

Harmonizing different jurisdictions' privacy or data protection laws becomes the key to facilitating cross-border data transfer. EU's adequacy decision approach serves this purpose unilaterally, which is powerful yet controversial. USMCA, CPTPP, DEPA, and RCEP pursue it through bilateral means with the assistance of international

---

[44] For instance, China applied to join DEPA on November 1, 2021. Ministry of Commerce People's Republic of China, *China has submitted an official application to join the Digital Economy Partnership Agreement (DEPA)* (Nov. 3, 2021), http://english.mofcom.gov.cn/article/newsrelease/significantnews/202111/20211103214781.shtml. However, no clue suggests that China would amend its existing restrictions on cross-border data transfer for the purpose of joining DEPA.

[45] Communications from the European Union, *Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce*, ¶ 2.8(2), INF/ECOM/22 (Apr. 26, 2019).

standards, but its real progress remains limited. DEPA further highlights the potential role of national trustmarks, but the actual operation of national trustmarks might return to the unilateral approach.[46] In sum, the unilateral approach risks arbitrariness, while the bilateral approach can hardly achieve real progress in practice.

IV. The Global CBPR Framework's Novel Approach

A novel approach has recently emerged parallel to the above efforts to harmonize privacy laws among different countries. As mentioned, APEC's CBPR System gained some attention in the USMCA. Recently, member economies to APEC's CBPR System have further expanded the APEC's CBPR System into the Global CBPR Framework. Below, I introduce CBPR's overall structure, features, and current achievements.

A. The Brief History of the Global CBPR Framework

The Global CBPR Framework originates from APEC's CBPR System, which is based on the APEC Privacy Framework. The APEC Privacy Framework was endorsed by APEC Ministers in 2005[47] and updated in 2015,[48] which lays down nine principles for ensuring information privacy, including preventing harm, notice, collection limitations, use of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability.[49] It also identifies itself as consistent with the core values of the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data.[50]

In the International Implementation Part of the 2005 APEC Privacy Framework, APEC economies committed to "endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with all applicable law."[51] They also committed to "endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable crossborder data transfers and effective privacy protections without creating unnecessary barriers to

---

[46] For instance, the EU adopts a national trustmark mechanism, i.e., the approved certification system, to serve as a basis alternative to the adequate decision for cross-border data transfer and designates the Europrivacy Certification as the EU's "national trustmark." However, Europrivacy Certification is regulated solely by the EU, rendering it dominated by the EU. Therefore, this approved certification system remains being operated in a unilateral approach.

[47] APEC, APEC PRIVACY FRAMEWORK (2005), https://www.apec.org/docs/default-source/publications/2005/12/apec-privacy-framework/05_ecsg_privacyframewk.pdf.

[48] APEC, APEC PRIVACY FRAMEWORK (2015), https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1.

[49] *Id.* Part III.

[50] *Id.* ¶ 5.

[51] APEC Privacy Framework (2005), *supra* note 47, ¶ 46.

cross-border information flows…."[52] These commitments were the foundation for APEC to build the CBPR System to balance privacy protection and cross-border data transfer.

In 2011, APEC Leaders endorsed APEC's CPBR System, which envisages a voluntary and accountability-based system to facilitate privacy-respecting data flows among APEC economies.[53] In general, APEC's CBPR System recognized the difficulties in obtaining consensus among members and, therefore, did not adopt a set of hard law regulations, like the GDPR, to discipline states' privacy rules.[54] Instead, it provides a more flexible "certification system" aimed at "organizations," assisting them to demonstrate their compliance with the privacy "principles" laid out by the APEC Privacy Framework by participating in the system.[55] In a sense, APEC's CBPR System adopts a bottom-up approach designed to harmonize organizations' privacy standards as a basis for further harmonizing domestic legislation.

APEC's CBPR System also makes it clear that it creates neither any obligations for APEC economies nor any obligations or expectations for non-participating governmental agencies.[56] In other words, APEC economies may determine whether to join this system voluntarily. As of July 2024, nine economies have participated in APEC's CBPR system, i.e., the United States, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei, and the Philippines.[57]

In 2022, seven of the above nine participating economies, excluding Australia and Mexico, announced the Global Cross-Border Privacy Rules Declaration, which extends the CBPR rules beyond APEC economies.[58] Based on the APEC's CBPR System, they established the Global CBPR Forum to introduce a global certification system open to any jurisdiction accepting the objectives and principles of the Global CBPR Forum.[59] In 2023, the Global CBPR Forum established the Global CBPR Framework, including the Global CBPR System applicable to data controllers and the Global Privacy Recognition for Processors ("PRP") System applicable to data processors.[60] Therefore, the Global CBPR Framework is no longer exclusive to APEC economies. In June 2023,

---

[52] *Id.* ¶ 48.
[53] *About CBPRs*, CBPRs, https://cbprs.org/about-cbprs (last visited Aug. 11, 2024).
[54] Peng, *supra* note 5, at 10.
[55] *Id.* at 7.
[56] CHARTER OF THE APEC CROSS-BORDER PRIVACY RULES AND PRIVACY RECOGNITION FOR PROCESSORS SYSTEMS JOINT OVERSIGHT PANEL, art. 1.1(i) and (iv).
[57] CBPR, Government, https://cbprs.org/government/ (last visited Aug. 11, 2024).
[58] GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) DECLARATION (Apr. 21, 2022), https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Declaration-2022.pdf.
[59] *Id.* ¶ 5.
[60] GLOBAL CBPR FORUM, GLOBAL CROSS-BORDER PRIVACY RULES AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS SYSTEMS: POLICIES, RULES AND GUIDELINES ["GLOBAL CBPR SYSTEMS POLICIES"] ¶ 2 (2023).

the United Kingdom participated in the Global CBPR System as an Associate.[61]

B. The Global CBPR Framework and Accountability Agents

CBPR's main feature is introducing a data privacy certification system aimed at "organizations" instead of "states." To elaborate, it recognizes that adequate privacy protection should be the prerequisite for cross-border data transfer and thus aims to ensure the privacy protection level when organizations transfer personal data across borders. By introducing a government-backed certification system at a global level, organizations may obtain certification by adhering to the privacy protection standards set by CBPR and thus demonstrate their compliance with globally recognized data privacy protections.[62] The certification received under this system, in turn, may serve as a basis for these organizations to conduct cross-border data transfer between CBPR members with fewer legal obstacles. The certification may also provide a means for organizations to obtain the public's trust in their privacy protection level when conducting cross-border data transfer.[63]

At CBPR's core are the Accountability Agents ("AAs"). AAs are the certification bodies recognized by the Global CBPR Forum to certify organizations' privacy protection practices, which can be private entities or governmental agencies. Organizations that wish to be certified as CBPR-compliant shall implement their data protection and privacy policies and practices consistent with the Global CBPR System Program Requirements, subject to an AA's compliance evaluation. AAs will evaluate whether to award the certification based on the Global CBPR or PRP Program Requirements.[64] Certified organizations will be published on the Global CBPR Forum website.[65]

AAs will further conduct ongoing monitoring and compliance review processes of the certified organizations. These processes include the notification and verification of the required corrections, annual attestation requirements, re-certification, and dispute resolution processes.[66] Furthermore, AAs will have mechanisms for enforcing Global CBPR Program Requirements through contract or by law. They may impose penalties against noncompliant organizations, such as terminating the certification, temporarily suspending the certification, publicizing the noncompliance practices of the

---

[61] *See* GLOBAL FORUM ASSEMBLY CHAIR, ANNUAL REPORT ["CBPR FORUM 2024 ANNUAL REPORT"] 2 (2024).
[62] *What is the Cross-Border Privacy Rules System*, APEC, https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system (last visited July 27, 2024).
[63] GLOBAL CBPR SYSTEMS POLICIES, *supra* note 60, ¶ 3.
[64] GLOBAL CBPR FORUM, ACCOUNTABILITY AGENT RECOGNITION APPLICATION, ANNEX A: ACCOUNTABILITY AGENT RECOGNITION CRITERIA ["AA RECOGNITION CRITERIA"], ¶¶ 4-5 (2023).
[65] GLOBAL CBPR SYSTEMS POLICIES, *supra* note 60, ¶ 15.
[66] AA RECOGNITION CRITERIA, *supra* note 64, ¶¶ 6-10.

organization, referring the violation to relevant privacy enforcement authorities, or imposing monetary penalties.[67] These mechanisms ensure the bindingness and integrity of certified organizations' privacy protection policies and practices.

AAs are, in turn, scrutinized by the Global CBPR Forum in at least the following two aspects. First, in conducting their certification, AAs must comply with the Recognition Criteria designed by the Global CBPR Forum, which covers their program requirements, dispute resolution procedures, policies and procedures for the avoidance of conflicts of interest, and other procedural issues such as the certification and re-certification processes, ongoing monitoring and compliance reviews, and enforcement of program requirements.[68] In other words, AAs must conduct their certification based on the criteria set by CBPR members. To be sure, these criteria are framed in general principles, thereby leaving a certain level of discretion for AAs to formulate their specific certification standards.

Second, AAs must obtain recognition from the Global CBPR Forum. To become a recognized AA, the applicant must first be nominated by a CBPR member and then reviewed and recommended by the AA Oversight and Engagement Committee ("AA Committee") established under the Global CBPR Forum for the Global Forum Assembly's consensus decision.[69] Any member may reject an application based on the applicant AA's failure to meet any criteria required for AA recognition.[70] Therefore, AAs are not purely private certification bodies but certification bodies backed by CBPR members.

Based on this novel AA design, CBPR features a delegated two-tier model for facilitating cross-border data transfer between members, under which CBPR members recognize AAs and agree on the general principles or guidance for AAs to conduct certification. At the same time, AAs certify the organizations and monitor their compliance with CBPR requirements. The relationship between CBPR members, accountability agents, and certified organizations may be described as follows:

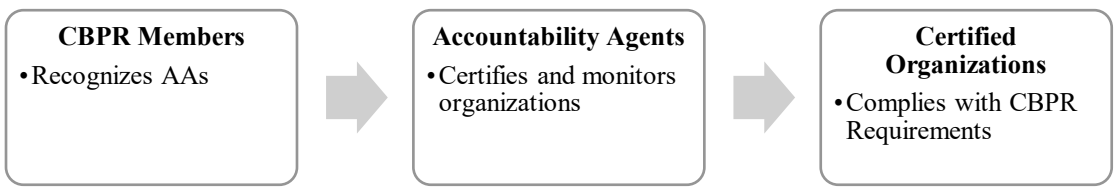


Chart 1: The Overview of the Global CBPR Framework

[67] *Id.* ¶¶ 11-14.
[68] GLOBAL CBPR SYSTEMS POLICIES, *supra* note 60, ¶ 17. *See also* AA RECOGNITION CRITERIA.
[69] GLOBAL CBPR SYSTEMS POLICIES, *id.* ¶¶ 33-39.
[70] *Id.* ¶ 43.

C. Current Progress of the Global CBPR Framework

On April 30, 2024, the Global Forum Assembly appointed AAs and recognized all eight APEC-recognized AAs to operate in their jurisdictions.[71] The eight AAs under the Global CBPR Framework are as follows:

Table 1: AAs under the Global CBPR Framework

Countries	Name of AAs
United States (4)	· BBB National Programs · NCC Group · Schellman · TRUSTArc
Japan (1)	· Japan Institute for Promotion of Digital Economy and Community
Republic of Korea (1)	· Korea Internet Security Agency
Singapore (1)	· Infocomm Media Development Authority
Chinese Taipei (1)	· Institute for Information Industry

While these AAs have not officially certified any organizations under the Global CBPR Framework, the Global Forum Assembly planned to start issuing Global CBPR and PRP certifications by these recognized AAs in the summer of 2024.[72] Foreseeably, certified organizations under the APEC's CBPR System will be the first batch receiving Global CBPR certifications. As of the end of July 2024, 75 organizations have received APEC's CBPR certification,[73] while 52 organizations have received APEC's PRP certifications,[74] including famous international enterprises such as Adobe, Apple, Cisco, General Electric, HP, Hyundai, Mastercard, Paypay, etc.

The majority of these certified organizations received their certifications from U.S.-based AAs. As the Table below exhibits, 51 certified CBPR organizations (or 68 percent) and 49 certified PRP organizations (or 94 percent) are certified by U.S.-based AAs. In comparison, AAs in Japan and Chinese Taipei relatively lag. Therefore, the United States businesses remain the primary CBPR users.

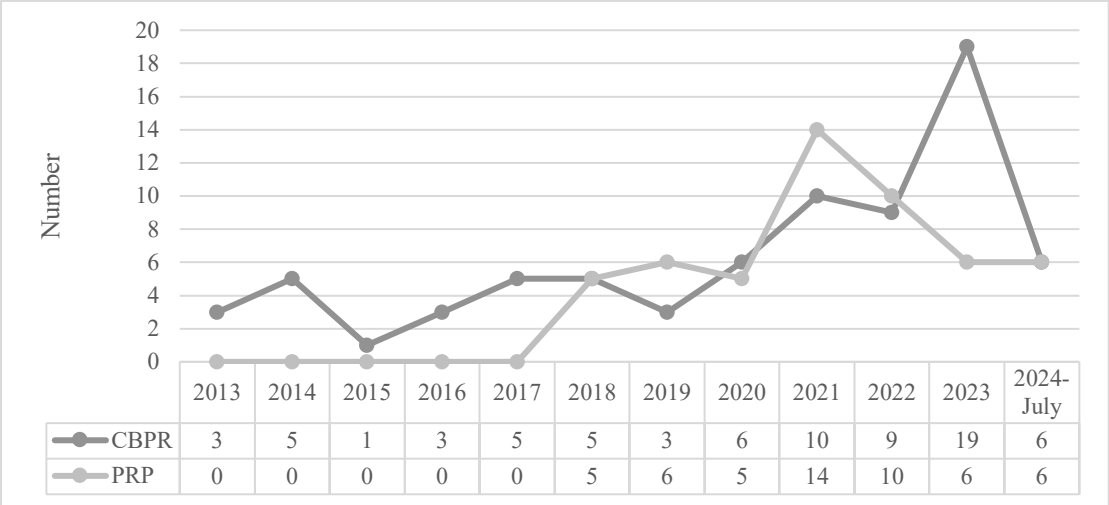
Table 2: Certified Organizations by APEC Economies

Countries	Name of AAs	CBPR No.	PRP No.
United States	BBB National Programs	6	3
	NCC Group	5	6
	Schellman	2	9
	TRUSTArc	38	31

[71] CBPR FORUM 2024 ANNUAL REPORT, *supra* note 61, at 1.
[72] *Id.* at 2.
[73] *See* CBPRs, *CBPR System Directory*, https://cbprs.org/compliance-directory/cbpr-system/ (last visited Aug. 11, 2024).
[74] *See* CBPRs, *PRP Directory*, https://cbprs.org/compliance-directory/prp/ (last visited Aug. 11, 2024).

Japan	Japan Institute for Promotion of Digital Economy and Community	4	0
Republic of Korea	Korea Internet Security Agency	13	0
Singapore	Infocomm Media Development Authority	6	3
Chinese Taipei	Institute for Information Industry	1	0

Chronologically, the number of certified organizations under APEC's CBPR System has gradually increased in recent years. As the chart below exhibits, an increasing number of organizations have obtained CBPR or PRP certifications since 2021, marking CBPR's growing popularity.



	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024-July
CBPR	3	5	1	3	5	5	3	6	10	9	19	6
PRP	0	0	0	0	0	5	6	5	14	10	6	6

Chart 2: Number of APEC's Certified Organizations by Year

Notably, the surge in recent years can be attributed to non-United States members. For instance, 20 of the 24 (or 83 percent) organizations certified by non-U.S.-based AAs received their certifications after 2021, contributing to 45 percent of the certifications during this period. This change demonstrates a more balanced development of APEC's CBPR System among its members.

In sum, APEC's CBPR System has made some achievements among businesses in this region in the past decade. Optimistically, this upward trend will be carried over to the Global CBPR Framework.

V. Some Reflections on the CBPR Approach

Existing CBPR studies seem less than positive due to CBPR's soft law nature. However, this chapter argues that CBPR adopts a novel soft law approach distinct from traditional soft law norms and, therefore, has the potential to harmonize the rules for

cross-border data transfer. This chapter also identifies CBPR's prospective challenges in the long run.

A. Theoretical Advantages of the CBPR Approach

CBPR's theoretical advantages lie in the following three aspects: the soft-law requirement at the state level, the public-private gatekeeper model at the global level, and the bottom-up approach for future harmonization.

a. The Soft-Law Requirement at the State Level

As most commentators observe, CBPR adopts a soft law approach for facilitating cross-border data transfer. Countries may voluntarily decide whether to participate in CBPR. Moreover, CBPR does not impose hard obligations on participating members and thus leaves broad discretion for members to formulate their domestic laws on cross-border data transfer. To be sure, CBPR members are obliged to align their domestic laws with the CBPR Framework.[75] However, to the extent that CBPR's substantive rules on privacy protection are framed in general principles, aligning domestic laws with the CBPR Framework should be less of a burden for most countries.

This soft-law approach aims to increase the global adoption of CBPR as much as possible. As mentioned, harmonizing different countries' privacy or data protection laws is the key to facilitating cross-border data transfer. To achieve this goal, more jurisdictions must be involved. Adopting a soft-law and principle-based regime makes CBPR less binding, which helps it garner more support in the first place.[76]

CBPR notes this aspect and carefully deals with the relationship between CBPR rules and domestic laws. On the one hand, it understands that most countries have privacy concerns about cross-border data transfer and, therefore, introduces its rules as a minimum privacy protection requirement for countries to participate. On the other hand, it notes that most countries prefer to preserve their right to regulate cross-border data transfer. Therefore, CBPR does not attempt to harmonize members' laws directly; it aims at something else.

b. The Public-Private Gatekeeper Model at the Global Level

CBPR's real harmonization effort targets the "standards" and "gatekeepers" for organizations to conduct cross-border data transfer, not the "laws" and "countries." In my view, this design artfully tackles the actual practice of cross-border data transfer.

---

[75] Global CBPR Forum Terms of Reference, Annex A, ¶ 3(a).

[76] James Y. Wang, *The Best Data Plan Is to Have a Game Plan: Obstacles and Solutions to Reaching International Data Privacy Agreements*, 28 MICH. TECH. L. REV. 385, 406 (2022).

The public policy concern against free cross-border data transfer centers around data privacy and security. To ensure that data controllers will protect data privacy and security, modern data laws impose a series of internal control requirements on data controllers, such as privacy by design/default and security requirements. After all, data controllers are the ones who withhold the data; therefore, they are expected to adopt "appropriate technical and organizational measures" to protect data privacy and security.

However, the sophistication of data technology prevents lawmakers and regulators from stipulating clear rules on these internal control requirements or enforcing them. For instance, lawmakers may find it impracticable to clearly define "appropriate" technical and organizational measures *ex-ante*. Even from an *ex-post* perspective, regulators or law enforcement may find it equally challenging to determine the appropriateness of the protection measures adopted by data controllers.

In practice, private certification bodies play an influential role in developing and enforcing internal control principles and rules for data privacy and security protection. For instance, the International Organization for Standardization ("ISO") is a representative data privacy and security certification body. ISO 27001 is perhaps one of the most widely adopted standards for information security management systems. ISO 27701, which focuses on standards for privacy information management, also obtained wide popularity in the industry. To be sure, data controllers are not legally obliged to observe these private standards. However, in practice, they prefer to obtain the certification issued by these authoritative certification bodies because it may signify their data privacy or security protection level, which helps expand their businesses.

Certifications play the above influential role in practice because of the inherent professional and informational asymmetry in the data industry. Data subjects are inherently at a disadvantageous position vis-à-vis data controllers because they are neither sophisticated in data technology nor aware of the data management practices adopted by data controllers. Similarly, regulators are also at a disadvantageous position vis-à-vis data controllers. By introducing a professional and trustworthy third party to establish data management standards and certify the data management measures adopted by data controllers, this "private gatekeeper" model alleviates the professional and informational asymmetry. This explains why the industry has gradually developed the practice of turning to authoritative certification bodies for certification.

CBPR injects more public elements into the private gatekeeper model and escalates it to a "public-private gatekeeper model." Under the private gatekeeper model, private certification bodies do not need a license to provide certification services. They also face minimal supervision and may formulate private standards for their initiatives.

CBPR, however, introduces a global licensing regime for its certification bodies. CBPR's certification bodies, i.e., the AAs, must obtain members' recognition to provide CBPR certification services. They also need to align their certification standards with CBPR's requirements. In short, CBPR's certification bodies are subject to a global level of disciplines and thus bear more public elements.

CBPR also goes further than the national trustmark highlighted in the DEPA. National trustmark generally refers to certification awarded by governmentally designated certification bodies, such as the Europrivacy Certification in the EU. CBPR's AAs go further in that they are recognized by not only a single country but all CBPR members. Therefore, their certification is recognized at a global level, which mitigates the unilateralism concern of national trustmark.

c. The Bottom-Up Approach for Future Harmonization

Mitigating the unilateralism concern is not the only advantage of adopting a public-private gatekeeper model at the global level for CBPR. CBPR's ultimate goal remains to harmonize the cross-border data transfer laws between countries, and the public-private gatekeeper model allows it to achieve this through a gradual and bottom-up approach.

As mentioned above, in practice, standards, instead of legislation, are the *de facto* rules governing the data management practices of data controllers. Suppose major data companies follow common standards and adopt similar data management practices. In that case, the need for countries to adopt divergent data legislation or restrict cross-border data transfer may be reduced. Therefore, by promoting more common data management standards and practices among members, CBPR envisages a bottom-up approach that may gear the convergence of data legislation in the future.

CBPR has achieved some progress in that aspect. Several members have adopted legislation that admits cross-border data transfer based on the CBPR certification. In Japan, Article 28 of the Personal Information Protection Act permits personal data transfer from Japan to a third country if the recipient in the third country has established and followed a system that meets the "standards prescribed by the Personal Information Protection Commission." These standards include cases where data recipients are certified according to relevant international frameworks for personal data processing.[77] According to the Personal Information Protection Commission's guidelines, CBPR's certification meets this condition.[78] In other words, Japan has incorporated CBPR's

[77] ENFORCEMENT REGULATIONS OF THE PERSONAL INFORMATION PROTECTION ACT (個人情報の保護に関する法律施行規則), art. 16 (Japan).

[78] GUIDELINES FOR THE PERSONAL INFORMATION PROTECTION ACT (PROVISION TO THIRD PARTIES IN

certification system into its domestic regime and permits cross-border data transfer out of Japan if the recipient is certified by AAs under the Global CBPR Framework.

Singapore is another good example. According to Article 10(1) of Singapore's Personal Data Protection Regulation, any organization transferring personal data overseas must ensure that the data recipient is bound by legal obligations equivalent to or higher than those in Singapore. According to Article 12 of the Regulation, this condition may be satisfied if the recipient holds the certification under APEC's CBPR System. Therefore, similar to Japan, Singapore has also incorporated CBPR certification into its domestic regime.

Japan's and Singapore's cases demonstrate the potential of CBPR's bottom-up approach. By its text, CBPR merely introduces a certification regime that parallels each member's domestic data regime. However, members may voluntarily incorporate the CBPR certification into their domestic data regimes to facilitate cross-border data transfer. If CBPR's certification gains recognition from all members, it may effectively serve as a single pass for cross-border data transfer between members. In that case, cross-border data transfer may be facilitated based on CBPR standards and certification despite the divergence in data laws between members.

B. Some Defenses of the CBPR Approach

The above illustration of CBPR's design and rationales may help rethink the associated critics of CBPR. To begin with, CBPR's soft law nature attracts some critics. Commentators often highlight CBPR's non-binding nature and call into question the public enforceability of its privacy rules.[79] However, as illustrated above, the soft law nature is crucial for enhancing CBPR's adoption. Moreover, CBPR also aims at a bottom-up approach to facilitate cross-border data transfer in a gradual manner. Once members voluntarily incorporate CBPR certification into their domestic regimes and recognize this global trustmark, such as Japan's and Singapore's cases, CBPR will become more binding. In this light, CBPR's soft law nature is a product of its gradual approach, which could be temporary.

Some commentators also expressed their doubts about CBPR's non-replacement nature. That is, CBPR principles go parallel to members' domestic regimes. Therefore, members may participate in CBPR while maintaining divergent domestic privacy laws, which cannot create a harmonized cross-border data transfer regime between

FOREIGN COUNTRIES) (個人情報の保護に関する法律についてのガイドライン(外国にある第三者への提供編)), ¶ 4-3 (Japan).

[79] Wang, *supra* note 76, at 406-07 (2022). *See also* Peng, *supra* note 5, at 9.

members.[80] However, as illustrated above, certification and standards are equally influential in actual practice. Therefore, CBPR aims to introduce a globally recognized certification system to facilitate cross-border data transfer without aligning each country's domestic legal regime. As illustrated above, once a country voluntarily recognizes the CBPR certification, cross-border data transfer may be facilitated, notwithstanding the divergent data laws between members.

Some commentators further pointed out that CBPR's privacy enforcement authorities, i.e., members' privacy regulators, did not adopt enforcement actions adequately, which may compromise CBPR's credibility.[81] To be sure, as of 2023, the United States Fair Trade Commission has adopted four CBPR-related enforcement actions,[82] including fining TRUSTe, an AA, for violating its certification policies by failing to timely re-certify the certified organizations in 2014.[83] Moreover, as some commentators have already noted, except for the U.S.-based AAs, Asia-based AAs are generally governmental or quasi-governmental bodies.[84] For those cases, regulators effectively have venues other than official disciplinary actions to ensure the sound operation of AAs.

In sum, CBPR adopts a gradual approach to balance cross-border data transfer and members' right to regulate. Therefore, it is inevitably soft and less interventionist for the present. However, if it can move in the optimistic direction, it could evolve into a more binding and effective regime.

C. Real Challenges of the CBPR Approach

In sum, despite the critics, I argue that CBPR has laid down a foundation with good rationales to foster cross-border data transfer. However, no system is perfect. Below, I enumerate CBPR's several challenges.

The first challenge is increasing its global adoption. As of July 2024, the Global CBPR Framework has nine members and one associate, which is a good start but needs further expansion. CBPR will need more members to reach the critical mass. Similarly, CBPR needs more organizations to join its certification system. The need to expand its global adoption is the primary reason CBPR should maintain its soft-law nature for the time being.

The second challenge is promoting more voluntary recognition. As illustrated

---

[80] Wang, *id.* at 407.
[81] Chander & Schwartz, *supra* note 5, at 97-99.
[82] FAIR TRADE COMMISSION, 2023 PRIVACY AND DATA SECURITY UPDATE 23 (2023).
[83] Peng, *supra* note 5, at 9.
[84] *Id.* at 8.

above, CBPR starts with a non-binding certification system but aims to elevate the system's legal status among members in the future. If more members voluntarily recognize the CBPR certification in their domestic regimes, CBPR's certification system will gradually become a cross-border data transfer pass. Therefore, members' voluntary recognition is the key to CBPR's future success.

Notably, considering the challenge of increasing global adoption, I would argue that CBPR should not pursue mandatory recognition by members, at least for the present. After all, requiring members to recognize CBPR certification will likely discourage non-members' participation. Therefore, at present, CBPR better follows the voluntary recognition design and focuses on how to encourage more members to recognize the CBPR certification domestically.

The third challenge is enforcing the data protection commitments. As some critics have raised, to create a globally credible data protection system, CBPR needs to enforce its privacy standards. While CBPR members delegate this mission to recognized AAs, they need to discipline these AAs to ensure an accountable certification system, which is CBPR's main difference from private certification systems. While CBPR's most prioritized topic might not rest on this accountability challenge, it should also not sidestep it.

VI. Conclusion

Cross-border data transfer is a crucial topic in modern digital trade law. The obstacle to promoting it results from the different mentalities of major countries and the resulting challenge of harmonizing data laws between different countries. Currently, most multilateral or regional efforts to promote cross-border data transfer attempt to create some principles or commitments at the state-to-state level. However, considering the lack of trust and shared values between countries under the existing geopolitical economy, I argue that these attempts will foresee significant challenges.

In this chapter, I review and comment on the design of the Global CBPR Framework, which takes a different state-to-gatekeeper approach that creates a global certification system. Despite the criticisms of its soft-law nature, I argue that CBPR's nonbinding design is needed to expand its global adoption. I illustrate how CBPR's design introduces a more inclusive, practical, and less interventionist approach to coordinating certification standards for cross-border data transfer at the gatekeeper level. I also highlight how this design envisages a bottom-up approach to promote recognition at the state level and creates a single pass in the long run. While CBPR's future success remains to be observed, its design rationales deserve more studies from an academic perspective.