Recommendations for Restoration of a Rules-Based International Trading System by the Research Group on the International Trading System led by the Japan Economic Foundation

Chapter 1 Restoration & Enhancement of WTO Functions
Section 2 Enhancement of Legislative Functions Through Expansion of Plurilateral Agreements
1-2.2

International Rulemaking Concerning the Cross-Border Free Flow of Data


Kojiro Fujii Shunya Muromachi

Abstract

As the ICT revolution and digitalization have dramatically changed the landscape of international trade, the cross-border free flow of data has become one of the primary agendas of trade rules. This paper discusses recent international rulemaking concerning the cross-border free flow of data.

Section II briefly discusses two types of barriers to the free flow of data. The first type is cross-border data flow regulations, which directly regulate cross-border data transfer. The second type of regulation is local storage requirements, which require the data to be stored in the territory of the state. **Section III** then addresses the developments of rules in Regional Trade Agreements (RTAs). The CPTPP is the first agreement establishing comprehensive, in-depth norms to address key issues related to the digital economy, including the two types of barriers to the free flow of data. The new provisions in the Japan-EU EPA, which entered into force on July 1, 2024, focus on building the ecosystem of data flows between Japan and the EU. **Section IV** explains the development of the Data Free Flow with Trust (DFFT) initiative. The Institutional Arrangement for Partnership (IAP) for the operationalization of the DFFT aims to create a single international, multi-stakeholder organization to coordinate the discussions on the DFFT that are advanced in various forums. Finally, **Section V** summarizes recent developments in the area of government access to privately held data, which is one of the priorities of the DFFT initiative. The OECD Government Access Declaration, which contains seven principles for trusted government access to data, can play a significant role despite its non-binding nature. In the meantime, there are developments in the system for a country to access

data located outside of its territory for law enforcement purpose, at the unilateral, bilateral and multinational levels.

While the free flow of data is critical to international trade, it is much more than just a trade issue. It requires a careful balance between the economic benefits of trade, and the rights of individuals. Some fundamental principles such as the rule of law, due process, judicial independence and transparency, as reflected in the OECD Government Access Declaration, have the potential to promote cooperation between countries having different regulatory priorities. In that sense, international rulemaking regarding the free flow of data (or more broadly, regarding the digital economy) has the geopolitical potential to strengthen the alliance of countries embracing such fundamental principles.

I. Introduction

The information and communication technology (ICT) revolution has dramatically changed the landscape of international trade. According to Prof. Richard Baldwin, the ICT revolution transformed what he calls traditional "20th century trade" (i.e. trade that is dominated by goods made in factories in one nation and sold to customers in another) to "21st century trade" (i.e. trade that involves complex two-way flows of goods, ideas, technology, capital, and technicians between internationally unbundled factories and offices).[1] In addition, the ICT revolution (i) increased the scale, scope and speed of trade, (ii) changed how goods are traded, (iii) changed how services are produced and supplied, blurring the distinction between goods and services, and (iv) facilitated cross-border trade in services.[2]

To maximize the positive impact of the ICT revolution on trade, it is important to ensure the free flow of data across borders.[3] There is some misunderstanding that the free flow of data benefits

[1] Richard Baldwin, "21st Century Regionalism: Filling the Gap between 21st Century Trade and 20th Century Trade Rules" (2011) CEPR Policy Insight No. 56, CEPR Press <https://cepr.org/publications/policy-insight-56-21st-century-regionalism-filling-gap-between-21st-century-trade-and> accessed Dec. 13, 2024.

[2] Javier Lopez Gonzalez, "The impact of digitalization on trade" (techUK, Oct. 31, 2022) <https://www.techuk.org/resource/the-impact-of-digitalisation-on-trade-oecd.html> accessed Dec. 13, 2024.

[3] The "free flow of data" means that individuals and entities are able to transfer data from one country to another country without being hindered by cross-border data flow regulations or local storage requirements (see Section II).

only "Big-Tech" companies.[4] However, the free flow of data has much more impact than that: it benefits all sectors including agriculture, transportation and logistics, finance and manufacturing, by improving efficiency in R&D, market forecasting, safety, productivity, sales, regulatory compliance, inventory control, supply chains and post-sale service.[5] It is also crucial for micro, small and medium-sized enterprises.[6] In 2021, the Ministry of Economy, Trade and Industry (METI) of Japan conducted a survey on cross-border data transfer, and the result of this survey shows that the majority of companies that responded do transfer data obtained outside of Japan across national borders for the purpose of data analysis, data management or other purposes.[7]

Against this background, this essay discusses recent international rulemaking concerning the cross-border free flow of data. It first briefly explains the two types of barriers to the free flow of data: cross-border data flow regulations and local storage requirements (Section II). It then addresses the developments in trade rules in RTAs, focusing on the relevant provision in the CPTPP[8] and the new provisions in the Japan-EU EPA[9] (Section III). It then explains the development of the Data Free Flow with Trust (DFFT) initiative (Section IV), and the discussion on the government access to privately held data, which is one of the priorities in the DFFT initiative (Section V).

II. Barriers to the Free Flow of Data

There are two types of regulations that work as barriers to the cross-border flow of data (*Chart 1*). The first type is cross-border data flow regulations, which directly regulates cross-border data transfer. The restrictiveness of the regulations varies depending on the conditions imposed upon the data flow, which can be categorized into (i) *ex post* accountability, (ii) *ex ante* safeguards (such as adequacy decision, binding corporate rules and standard contractual clauses), and (iii) *ex ante* (ad

[4] Dan Dupont, "U.S. to end support for WTO e-commerce proposals, wants 'policy space' for digital trade rethink", *Inside US Trade* (Oct. 24, 2023) <https://insidetrade.com/share/178191> accessed Dec. 13, 2024.

[5] Global Data Alliance, "Jobs in All Sectors Depend Upon Data Flow" (March 2020) <https://globaldataalliance.org/wp-content/uploads/2021/07/infographicgda.pdf> accessed Dec. 13, 2024.

[6] International Chamber of Commerce, "ICC White Paper on Trusted Government Access to Personal Data Held by the Private Sector" (Aug. 22, 2022) <https://iccwbo.org/news-publications/policies-reports/icc-white-paper-on-trusted-government-access-to-personal-data-held-by-the-private-sector/> accessed Dec. 13, 2024, pp. 5-6.

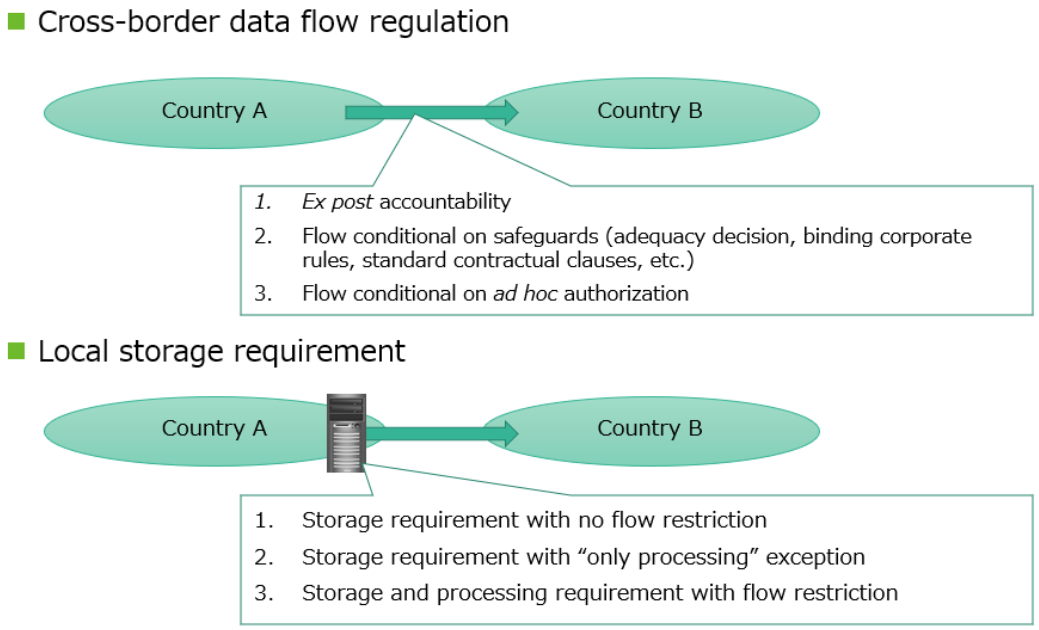
[7] METI, "Company Questionnaire on International Data Transfer and Utilization" (May 31, 2021) <https://www.meti.go.jp/press/2021/05/20210531001/20210531001.html> (available only in Japanese) accessed Dec. 13, 2024.

[8] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (Santiago, 2018).

[9] Agreement between the European Union and Japan for an Economic Partnership (Tokyo, 2018).

hoc) authorization.[10] The second type of regulation is local storage requirements, which requires the data to be stored in the territory of the state. This can be further categorized into (i) storage requirements with no flow restrictions, (ii) storage requirements with an "only processing" exception, and (iii) storage and processing requirement with flow restrictions.[11]

CHART 1 Types of barriers to the free flow of data



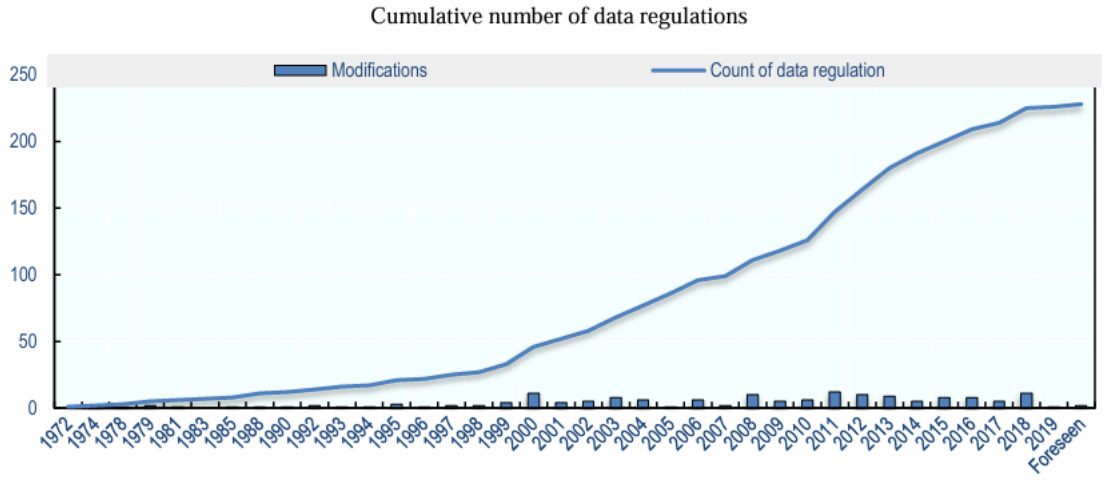
Source: Compilation, based on Casalini & González (2019)

The following *Chart 2* indicates that the number of cross-border data regulations and local storage requirements has constantly increased.

[10] Francesca Casalini and Javier López González, "Trade and Cross-Border Data Flows" (2019) OECD Trade Policy Papers, No. 220, OECD Publishing < https://doi.org/10.1787/b2023a47-en > accessed Dec. 13, 2024, pp. 16-17.

[11] ibid, pp. 23-24.

CHART 2 Number of cross-border data flow regulations & local storage requirements



Note: Data protection regulations include different types of regulation relating to data transfers and local storage requirements. Numbers are affected by the way in which regulations are structured, as this varies by country; some countries may have a single regulation covering a wide range of measures; others will have several different regulations covering, for example, restrictions on data flows for different types of data, and local storage requirements.

Source: Casalini & González (2019), p. 15

These regulations are introduced for various purposes, such as personal data protection, security-related data protection, law enforcement and surveillance or digital industrial policy.[12]

These measures have a significant impact on trade. According to González and Kaynak (2023), the prohibition of the free flow of data increases the export costs in all sectors in many countries.[13] In addition, Giovane, Ferencz and González (2023) conducted a survey covering cross-border e-payments, cloud computing and air travel, and identified that local storage requirements, including those without free flow restrictions, have a negative impact on businesses as well as downstream players relying on those businesses, competition and cybersecurity.[14]

---

[12] ibid, p. 14.

[13] López González, J., S. Sorescu and P. Kaynak, "Of bytes and trade: Quantifying the impact of digitalization on trade" (2023), OECD Trade Policy Papers, No. 273, OECD Publishing <https://doi.org/10.1787/11889f2a-en> accessed Dec. 13, 2024, pp. 26-27.

[14] Del Giovane, C., J. Ferencz and J. López González, "The Nature, Evolution and Potential Implications of Data Localisation Measures" (2023), OECD Trade Policy Papers, No. 278, OECD Publishing, Paris, <https://doi.org/10.1787/179f718a-en> accessed Dec. 13, 2024.

III. Development of International Trade Rules for the Free Flow of Data

In the past 10 years, there have been significant developments in international trade rules to promote the free flow of data. Some of the WTO Agreements apply to matters pertaining to the digital economy, including free flow of data. In particular, many commentators have pointed out that the General Agreement on Trade in Services (GATS)[15] plays an important role in the promotion of the free flow of data.[16] However, as discussed in our introduction, the free flow of data relates to all sectors, not just the services sector. In addition, due to the cross-sectional nature of digital services, it is difficult to determine whether each member country's specific commitment under the GATS applies to the restriction on the free flow of data in question.[17] The participants of the Joint Statement Initiative (JSI) on Electronic Commerce, a plurilateral initiative for negotiations on trade-related aspects of electronic commerce,[18] have negotiated provisions for the free flow of data, but due to their controversial nature,[19] the participants have not been able to agree on them. On July 26, 2024, the co-conveners of the JSI (Japan, Australia and Singapore) issued a joint statement accompanied with the stabilized text of the Agreement on Electronic Commerce, [20] but provisions for free flow of data were not included in that text. [21]

In the meantime, countries have begun to conclude RTAs which narrowly and explicitly establish rules for important issues concerning digital economies. According to the Trade Agreement

---

[15] General Agreement on Trade in Services (Marrakesh, 1994).

[16] For example, Andrew D. Mitchell and Jarrod Hepburn, "Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017), 19 *Yale Journal of Law and Technology*.

[17] Andrew D Mitchell and Neha Mishra, "WTO Law and Cross-Border Data Flows: An Unfinished Agenda" in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press 2021), p. 93.

[18] WTO, "Joint Statement Initiative on E-commerce" <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm> accessed Dec. 13, 2024.

[19] For example, China has expressed its position that "the data flow should be subject to the precondition of security, which concerns each and every Member's core interests". WTO, "Joint Statement on Electronic Commerce: Communication from China" INF/ECOM/19 (2024), para 4.3. The United States used to support provisions on free flow of data and data localization, but withdrew its support in October 2023 in order to ensure sufficient "policy space" to regulate Big Tech companies. Dupont (Note 4).

[20] WTO, "Joint Statement Initiative on Electronic Commerce: 26 July 2024" INF/ECOM/87 (2024).

[21] However, provisions such as Article 5 (Electronic Authentication and Electronic Signatures), Article 16 (Personal Data Protection) and Article 17 (Cybersecurity) could function as a foundation of building trust in the data flows between the WTO members.

Provisions on Electronic-commerce and Data (TAPED) dataset (updated Nov. 20, 2024), compiled by Prof. Mira Burri and her team, the number of such agreements has exceeded 465.[22]

The CPTPP was the first important attempt to establish comprehensive, in-depth norms to address key issues concerning the digital economy, including the free flow of data, on a significant scale. The key achievements of the CPTPP have been followed by slight variations in subsequent important RTAs such as the USMCA,[23] the Japan-US DTA[24] and the Japan-UK EPA.[25]

The CPTPP contains two important provisions for the free flow data. The first provision is Article 14.11 (Cross-Border Transfer of Information by Electronic Means), which concerns cross-border data flow regulations. Paragraph 2 requires the contracting parties to allow cross-border data transfer for the conduct of business of a covered person.[26] On the other hand, paragraph 3 provides that the contracting parties can introduce measures inconsistent with paragraph 2 to achieve legitimate public policy objectives, provided that such measures (i) are not applied as a means of discrimination or a disguised restrictions on trade, and (ii) do not impose restrictions on data transfer greater than necessary to achieve their objectives. The second provision is Article 14.13 (Location of Computing Facilities), which concerns local storage requirements. Paragraph 2 of that provision prohibits contracting parties from requiring a covered person to use or locate computing facilities in their territory as a condition for conducting business in their territory, but paragraph 3 provides an exception for legitimate public policy measures, similar to Article 14.11, paragraph 3. The public policy exceptions in paragraph 3 of both Articles 14.11 and 14.13 provide contracting parties with certain policy space to regulate the flow of data.[27]

---

[22] University of Lucerne, "TAPED: A Dataset on Digital Trade Provisions" < https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/> accessed Dec. 13, 2024.

[23] Agreement between the United States of America, the United Mexican States, and Canada (Buenos Aires, 2018).

[24] Agreement between the United States of America and Japan concerning Digital Trade (Washington D.C., 2019).

[25] Agreement between the United Kingdom of Great Britain and Northern Ireland and Japan for a Comprehensive Economic Partnership (Tokyo, 2020).

[26] The term "covered person" means (i) an investment of an investor of a party, (ii) an investor of a party and (iii) a service supplier of a party, excluding financial service suppliers. CPTPP Article 14.1, referring to CPTPP Articles 9.1, 10.1 and 11.1.

[27] In addition, contracting parties are allowed to take measures that they consider necessary for the protection of essential security interests under Article 29.2(b).

The USMCA, the Japan-US DTA, and the Japan-UK EPA have provisions corresponding to CPTPP Articles 14.11 and 14.13.[28] These provisions (except for Japan-US DTA Article 11) exclude financial services from their scope. Instead, these agreements have separate provisions that cover financial services (*Table 1*). Among these four agreements, only the CPTPP does not have a provision specifically addressing local storage requirements applicable to financial services. USMCA Article 17.18, Japan-US DTA Article 13 and Japan UK-EPA Article 8.63 prohibit local storage requirements as long as the regulatory authority of each contracting party has effective access to information for regulatory or supervisory purposes.

TABLE 1 Data-related provisions & financial services

Agreement	Provision	Title of the Provision	Type of regulations concerned	Applies to financial services?
CPTPP	14.11	Cross-Border Transfer of Information by Electronic Means	Cross-border data flow regulation	No
	14.13	Location of Computing Facilities	Local storage requirement	No
	Annex 11-B, Section B	Transfer of Information	Cross-border data flow regulation	Yes
USMCA	19.11	Cross-Border Transfer of Information by Electronic Means	Cross-border data flow regulation	No
	19.12	Location of Computing Facilities	Local storage requirement	No
	17.17	Transfer of Information	Cross-border data flow regulation	Yes
	17.18	Location of Computing Facilities	Local storage requirement	Yes
JP-US DTA	11	Cross-Border Transfer of Information by Electronic Means	Cross-border data flow regulation	Yes
	12	Location of Computing Facilities	Local storage requirement	No
	13	Location of Financial Service Computing Facilities for Covered Financial Service Suppliers	Local storage requirement	Yes
JP-UK EPA	8.84	Cross-Border Transfer of Information by Electronic Means	Cross-border data flow regulation	No
	8.85	Location of Computing Facilities	Local storage requirement	No
	8.63	Financial Information	Cross-border data flow regulation/ Local storage requirement	Yes

Source: Authors' compilation

In addition to the aforementioned agreements, Japan and the EU have recently agreed on new provisions on data flows, which entered into force on July 1, 2024.[29] The Japan-EU EPA did not have provisions on data flows in its e-commerce section (Chapter 8, section F) when it was originally signed in July 2018. Instead, Article 8.81 provided that the contracting parties will reassess the need

[28] USMCA Articles 19.11 and 19.12; JP-US DTA Articles 11 and 12; Japan-UK EPA Articles 8.84 and 8.85. There are some differences between these provisions. For example, USMCA Article 19.12 and JP-US DTA Article 12 (both on location of computing facilities) do not include a public policy exception corresponding to CPTPP Article 14.13, paragraph 3 (while USMCA Article 19.11 and JP-US DTA Article 11 include it).

[29] Protocol Amending the Agreement between the European Union and Japan for an Economic Partnership (Brussel, 2024); European Union, "EU-Japan deal on data flows enters into force" (July 1, 2024) <https://policy.trade.ec.europa.eu/news/eu-japan-deal-data-flows-enters-force-2024-07-01_en> accessed Dec. 13, 2024.

for inclusion of the free flow of data into the Japan-EU EPA within three years. The European Commission had published the "Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection EU Trade and Investment Agreements" in February 2018,[30] but its content was very different from the content of CPTPP-type provisions which have been endorsed by Japan.

The new provisions in the Japan-EU EPA are mainly comprised of the new Article 8.81 (Cross-border transfer of information by electronic means) and the new Article 8.82 (Protection of personal data). The new Article 8.81, paragraph 2 (*Table 2*) provides a list of measures that the contracting parties are not allowed to adopt or maintain. It is similar to Article A, paragraph 1 of the European Commission's Horizontal Provisions, but subparagraphs (e) (prohibiting the transfer of information into the territory of the party) and (f) (requiring the approval of the party prior to the transfer of information to the territory of the other party) were added. Subparagraphs (c), (e) and (f) cover cross-border data flow regulations, but they only cover transfer of data to "the territory of the (other) Party". They are narrower than CPTPP Article 14.11, paragraph 2, which requires contracting parties to allow cross-border data transfers, regardless of their destinations. On the other hand, subparagraphs (a), (b) and (d) cover local storage (and processing) requirements. They are broader than CPTPP Article 14.13, paragraph 2 because subparagraph (a) covers the use of not only "computing facilities", but also "network elements".[31]

[30] European Commission, "Horizontal provisions on cross-border data flows and personal data protection" (May 18, 2018) <https://ec.europa.eu/newsroom/just/items/627665> accessed Dec. 13, 2024.

[31] EU-Lex, "Protocol amending the Agreement between the European Union and Japan for an economic partnership" <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22024A01304> accessed Dec. 13, 2024.

TABLE 2 Text of the new Article 8.81, paragraph 2

2. To that end, a Party shall not adopt or maintain measures which prohibit or restrict the cross-border transfer of information set out in paragraph 1 by:

(a) requiring the use of computing facilities or network elements in the territory of the Party for information processing, including by requiring the use of computing facilities or network elements that are certified or approved in the territory of the Party;

(b) requiring the localisation of information in the territory of the Party for storage or processing;

(c) prohibiting storage or processing of information in the territory of the other Party;

(d) making the cross-border transfer of information contingent upon use of computing facilities or network elements in the territory of the Party or upon localisation requirements in the territory of the Party;

(e) prohibiting the transfer of information into the territory of the Party; or

(f) requiring the approval of the Party prior to the transfer of information to the territory of the other Party (1).

Source: EU-Lex, "Protocol amending the Agreement between the European Union and Japan for an economic partnership" <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22024A01304> accessed Dec. 13, 2024.

The new Article 8.81 is also different from CPTPP Articles 14.11 and 14.13 in terms of the scope of measures that the contracting parties can adopt or maintain (*Table 3*). First, paragraph 3 provides an exception for measures for legitimate public policy objectives that is similar to paragraph 3 of CPTPP Articles 14.11 and 14.13, but with a footnote stating that "legitimate public policy objective" shall be interpreted in an objective manner. In addition, paragraph 4 provides an exception specifically for measures on the protection of personal data and privacy. This paragraph is similar to Article B, paragraph 2 of the European Commission's Horizontal Provisions, but different as it does not use the self-judging language in Article B, paragraph 2 ("it deems appropriate") and provides certain conditions for the measures to be justified ("provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the information transferred").[32]

[32] In addition to the above, footnote 1 to the new Article 8.81 clarifies that the subparagraph 2(f) does not prevent measures that are justified under paragraphs 3 or 4 or other exceptions applicable to the new Article 8.81 (security exceptions, general exceptions and prudential carve out).

TABLE 3 Text of the new Article 8.81, paragraphs 3 & 4

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraphs 1 and 2 to achieve a legitimate public policy objective ([2]), provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information that are greater than necessary to achieve the objective. ([3])

4. Nothing in this Article shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border transfers of information, provided that the law of the Party provides for instruments enabling transfers under conditions of general application ([4]) for the protection of the information transferred.

Source: EU-Lex (Note 31)

The new Article 8.82 requires contracting parties to adopt or maintain a legal framework that provides for the protection of personal data related to electronic commerce in paragraph 3. The new Article 8.82 is similar to CPTPP Article 14.8, but there are some differences. First, paragraph 1 includes a recognition individuals' right to the protection of their personal data and privacy, similar to Article B, paragraph 1 of the European Commission's Horizontal Provisions. Second, paragraph 1 also includes a recognition that each contracting party has the right to determine the appropriate level of protection of personal data and privacy. This could serve as a context to justify strict measures for the protection of personal data and privacy, under the new Article 8.81, paragraph 4. Finally, paragraph 3 includes a recognition that "high standards of privacy and data protection as regards government access to privately held data" contributes to "trust in the digital economy", and specifically refers to "the OECD Principles for Government Access to Personal Data held by Private Sector Entities" as an example of such high standards. As explained in the next section, the issue of government access to privately held data is considered to be one of the most important issues in the DFFT discussions, and these provisions appear to reflect such trends.

The difference between the CPTPP and the new provisions in the Japan-EU EPA can be summarized as follows. The new Article 8.81 is designed to promote the free flow of data only between Japan and the EU, while CPTPP Article 14.11 and 14.13 covers barriers to free flow of data that may affect the business of the covered persons regardless of destination of data. In that sense, the new provisions focus on building the ecosystem of data flows between Japan and the EU. The new provisions incorporate exceptions beyond those provided in paragraph 3 of CPTPP Articles 14.11 and 14.13 (legitimate public policy) such as those in Article B, paragraph 2 of the European Commission's Horizontal Provisions (protection of personal data and privacy) with stricter disciplines on the

contracting parties' discretions. The new Article 8.82 is similar to CPTPP Article 14.8, but it reflects the shared understanding of Japan and the EU regarding the protection of personal data, including the recognition of individuals' right and the importance of high standards regarding government access to privately held data.

Japan and the EU have already promoted the free flow of personal data by a mutual adequacy arrangement based on their respective domestic regulations,[33] but there is no international law obligation to maintain this arrangement. The new provisions in the Japan-EU EPA will provide more predictability for the business operators in Japan and the EU, by stabilizing the mutual adequacy arrangement on personal data and by preventing the introduction of excessive barriers to the free flow of data (including non-personal data) between Japan and the EU.

IV. Developments towards the DFFT

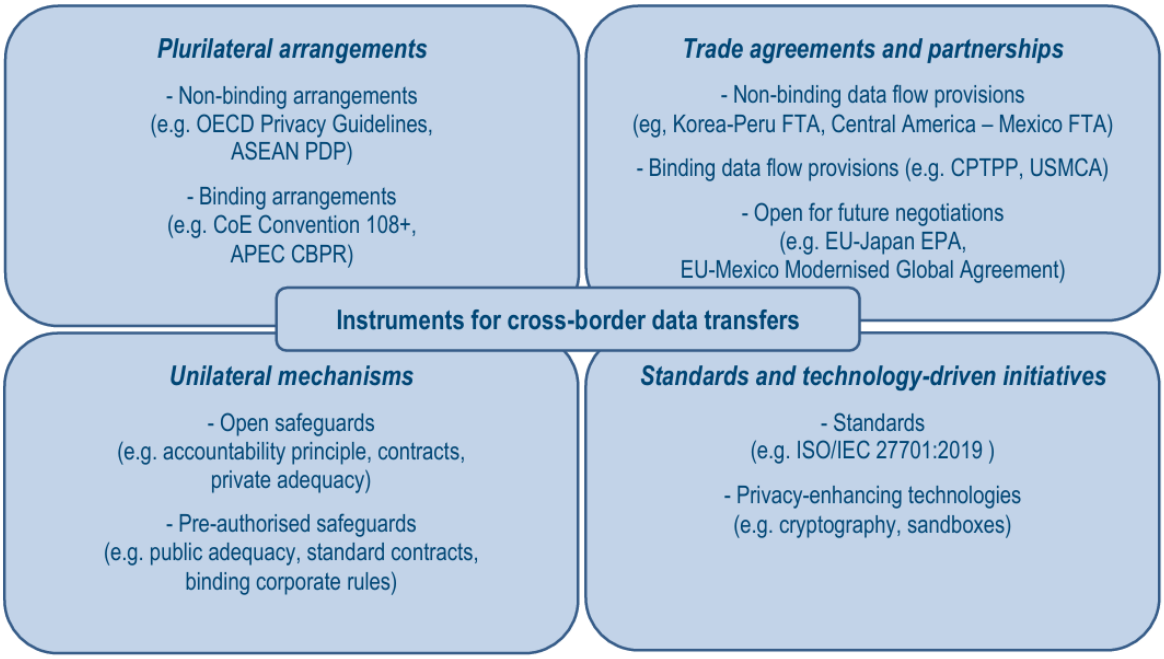
While free flow of data is essential to trade, trade agreements are not the only approach to addressing the flow of data. Every country has its own interest in regulating the flow of data, sometimes linked to the notion of "data sovereignty", and such interests often have tension with the concept of the free flow of data.[34] Countries address the issue of cross-border data transfer in their domestic regulations (unilateral measures), or sometimes through plurilateral regulatory mechanisms such as the Cross-Border Privacy Rules (CBPR) systems based on the APEC Privacy Principles. Casalini, González and Nemoto (2021) provide a comprehensive overview of instruments for cross-border data transfers, including trade agreements (*Chart 3*).[35]

[33] Personal Information Protection Commission. "The framework for mutual and smooth transfer of personal data between Japan and the European Union has come into force" <https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/> accessed Dec. 13, 2024.

[34] Neha Mishra, *International Trade Law and Global Data Governance: Aligning Perspectives and Practices* (Hart 2024), pp. 45-49.

[35] Casalini, F., J. López González and T. Nemoto, "Mapping commonalities in regulatory approaches to cross-border data transfers" (2021), OECD Trade Policy Papers, No. 248, OECD Publishing <https://doi.org/10.1787/ca9f974e-en> accessed Dec. 13, 2024, pp. 12-13.

CHART 3: Mapping of the Instruments for cross-border data transfers



Source: Casalini, González and Nemoto (2021), p. 12.

In light of the above, the discussion on the free flow of data should not be limited to the "trade track", but should also involve the "regulatory track", and the concept of DFFT provides the link between these two tracks.[36] This concept was proposed by former Prime Minister Shinzo Abe at the World Economic Forum Annual Meeting in 2019,[37] and aims to promote the free flow of data while ensuring "trust" in privacy, security, and intellectual property rights.[38] Prof. Neha Mishra comments that the flexibility of the concept of the DFFT provides "an inherent advantage in dealing with several of the existing legal and policy uncertainties in global data governance and digital trade".[39]

---

[36] Aidan Arasasingham and Matthew P. Goodman, "Operationalizing Data Free Flow with Trust (DFFT)" (CSIS, April 13, 2023) <https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft> accessed Dec. 13, 2024, p. 3.

[37] Ministry of Foreign Affairs of Japan, "Speech by Prime Minister Abe at the World Economic Forum Annual Meeting: Toward a New Era of 'Hope-Driven Economy'" (23 January 2019) <https://www.mofa.go.jp/ecm/ec/page4e_000973.html> accessed Dec. 13, 2024.

[38] Digital Agency of Japan, "Data Free Flow with Trust (DFFT)" <https://www.digital.go.jp/en/dfft-en> accessed Dec. 13, 2024.

[39] Mishra (Note 34), p. 19.

In the meeting in April 2023, the G7 Digital and Tech Ministers declared the establishment of the Institutional Arrangement for Partnership (IAP) to operationalize DFFT.[40] The purpose of the IAP is to create a single international, multi-stakeholder organization to coordinate the discussions on the DFFT advanced in various forums.[41]

The Ministerial Declaration in April 2023 also identifies four priority areas: (i) data localization; (ii) regulatory cooperation; (iii) trusted government access to data: and (iv) data sharing (*Table 4*).

TABLE 4 Four priority areas identified in the 2023 G7 Ministerial Declaration

Data Localization	Focus on understanding the impact of data localization measures while considering different data governance approaches and policy objectives.
Regulatory Cooperation	Identify commonalities in regulatory approaches, promote privacy-enhancing technologies (PETs), approaches, and access to regulatory information and practices.
Trusted Government Access to Data	Promote awareness of the OECD Government Access Declaration and develop risk-based approaches to preventing government access that is inconsistent with democratic values and the rule of law.
Data Sharing	Uphold the role of technology and use cases thereof, such as digital credentials and identities. Improved data use is a major strategic opportunity for economic growth.

Source: Compilation, based on the 2023 G7 Ministerial Declaration

While the first area (data localization) is the most relevant to the trade track, the other areas may also provide implications for trade rules. For example, as discussed in the previous section, the new Article 8.82 of the Japan-EU EPA refers to the OECD Government Access Declaration (discussed in the next section) as one of the "high standards of privacy and data protection as regards government access to privately held data" that contribute to trust in the digital economy. Conversely, trade rules may provide some implications for other policy areas. For example, the WTO Agreements and Regional Trade Agreements provide various mechanisms to improve transparency of measures

[40] G7 Digital and Tech Ministers' Meeting, "Ministerial Declaration" (Takasaki, April 30, 2023) para 13; G7 Digital and Tech Ministers' Meeting, "G7 Digital and Tech Track Annex 1 - Annex on G7 Vision for Operationalizing DFFT and its Priorities" (Takasaki, April 30, 2023).

[41] Arasasingham and Goodman (Note 36), p. 6.

affecting trade,[42] and the regulatory cooperation under the IAP can learn from these mechanisms to improve access to regulatory information and practices.[43]

The establishment of the IAP has been endorsed by the G7 leaders at the Hiroshima Summit 2023,[44] and it is currently taking the form of an expert community at the OECD.[45] In the Apulia Summit 2024, the G7 leaders recognized their common interest in ensuring the "highest standards for sensitive data protection and security, including genomic data",[46] and this may provide further context for the embodiment of the DFFT and thus become a priority area for the IAP.

V. The Issue of Government Access to Privately Held Data

As highlighted in the 2023 G7 Ministerial Declaration, the issue of government access to privately held data is critical for the promotion of the DFFT. There are two important links between this issue and the free flow of data.[47] First, because government access to private data negatively affects human rights, including the protection of personal data and privacy, countries (especially those with strong data protection regulations) do not allow the transfer of (personal) data to other countries or regions where there is arbitrary and non-transparent government access to data. For example, since the judgment of the Court of Justice of the European Union in the Schrems II case,[48] the European data protection authorities (DPAs) have strictly addressed the risks of access to European personal data by the intelligence and law enforcement agencies of foreign countries under Chapter V of the

---

[42] For example, GATS Article 12 requires members to publish or make publicly available information about measures that affect trade in services and to establish an enquiry point to provide specific information to other members upon request.

[43] Kojiro Fujii, Taku Nemoto and Atsunaka Fukushima, "Ensuring Transparency in Regulating Cross-Border Data Transfer: Building International Institution" in Yurika Ishii (ed) *Opening the Future of Information Law: New Issues in the Age of AI, National Security* (Houritsu Bunka Sha 2024), pp. 112-135. The essence is available at <https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/006_02_00.pdf> accessed Dec. 13, 2024 (available only in Japanese).

[44] G7 Hiroshima Summit 2023, "G7 Hiroshima Leaders' Communiqué" (Hiroshima, May 2023) paragraph 39.

[45] G7 Industry, Technology and Digital Ministerial Meeting, "Ministerial Declaration" (Verona and Trento, March 15, 2024) para. 11.

[46] G7 Apulia Summit 2024, "Apulia G7 Leaders' Communiqué" (Apulia, June 2024)

[47] Kojiro Fujii and Yurika Ishii, "Government Access to Data and International Cooperation toward Data Free Flow with Trust" in Dai Yokomizo, Yoshizumi Tōjō and Yoshiko Naiki (eds), *Changing Orders in International Economic Law: Volume 2: A Japanese Perspective* (Routledge 2024), p. 110.

[48] Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559.

General Data Protection Regulation (GDPR).[49] Businesses are also hesitant to transfer data to such countries or regions because such access will jeopardize their ability to protect their customers' persona data and privacy and to comply with applicable data protection laws.[50] Second, some countries introduce local storage requirements in order to ensure effective access to data for regulatory purposes, including law enforcement and investigation. For example, the Cyber Security Law of Vietnam requires certain service providers operating in Vietnam to store certain types of data with the territory of Vietnam. According to a decree implementing this local storage requirement, foreign service providers are also subject to this requirement, but only in cases where the service was used for a violation of the Cyber Security Law.[51]

With respect to the first link, the members of the OECD made a declaration titled "Declaration on Government Access to Personal Data Held by Private Sector Entities" in December 2020 (OECD Government Access Declaration).[52] This declaration contains seven principles for trusted government access to privately held personal data for law enforcement and national security purposes (*Table 5*). Although this declaration is non-binding, it can play a significant role by being incorporated in relevant international agreements (such as the new Article 8.82 of the Japan-EU EPA) or by being considered in the implementation of relevant domestic regulations.[53]

---

[49] Theodore Christakis, "The 'Zero Risk' Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach" (2024), CIPL/CBDF Paper Series <https://ssrn.com/abstract=4732294> accessed Dec. 13, 2024. The paper argues that the "zero risk" approach adopted by the DPAs is overly restrictive, and the DPAs should adopt a "risk-based" approach in interpreting Chapter V of the GDPR.

[50] International Chamber of Commerce (Note 6), p. 11.

[51] Decree No. 53/2022/ND-CP guiding certain articles of the Law on Cybersecurity, Article 53, paragraph 3.

[52] OECD, "Declaration on Government Access to Personal Data Held by Private Sector Entities" (Dec. 14, 2022) OECD/LEGAL/0487 (OECD Government Access Declaration).

[53] For example, the Guidelines on the Act on the Protection of Personal Information (for Transfers to Third Parties in Foreign Countries) published by the Personal Information Protection Commission refers to the OECD Government Access Declaration as a standard that business operators may refer to when assessing foreign government access measures.

TABLE 5 Seven principles in the OECD Government Access Declaration

1. Legal basis: Government access is provided for and regulated by the country's legal framework, which is binding on government authorities and is implemented by democratically established institutions operating under the rule of law. The legal framework sets out the purposes, conditions, limitations, and safeguards for government access, so that individuals have sufficient guarantees against the risks of misuse and abuse.
2. Legitimate aims: Government access supports the pursuit of specified and legitimate aims. Government access is carried out in a manner that is not excessive in relation to the legitimate aims. Governments do not seek access to personal data for the purpose of suppressing criticism or disadvantaging persons solely on the basis of characteristics, including, but not limited to: ethnicity, gender identity, expression, etc.
3. Approval: The legal framework establishes prior approval ("approval") requirements for government access, to ensure that access is performed in accordance with applicable standards, rules, and processes. The requirements are commensurate with the degree of interference with privacy and other human rights that will occur as a result of government access. Stricter approval requirements are in place for cases involving more serious interference.
4. Data handling: Personal data acquired through government access can be processed only by authorized personnel. This processing is subject to requirements, which include putting in place measures to maintain privacy, security, confidentiality, and integrity. Internal controls are put in place to prevent data loss or unauthorized data access.
5. Transparency: The general legal framework for government access is clear and easily accessible. Mechanisms exist for providing transparency about government access, and include public reporting by oversight bodies on government compliance with legal requirements and with procedures for requesting access to government records.
6. Oversight: Mechanisms exist for effective and impartial oversight, to ensure that government access complies with the legal framework. Countries' oversight systems are comprised of bodies with powers that include the ability to obtain relevant information, conduct investigations, and address non-compliance.
7. Redress: The legal framework provides individuals with effective judicial and non-judicial redress to identify and remedy violations of the national legal framework. These redress mechanisms take into account the need to preserve the confidentiality of national security and law enforcement activities. This may include limitations on the ability to inform individuals of whether their data was accessed or whether a violation occurred.

Source: Authors' compilation

With respect to the second link, the US and the EU have developed a system for orders to disclose or produce data located outside of their territory,[54] which can be an alternative to the local storage requirements to ensure effective law enforcement. These mechanisms include a system for resolving conflicts of law and a mechanism to enforce the order against entities outside of their jurisdiction (Table 6). While the US approach can be characterized as a "bilateral" approach through the conclusion of executive agreements, the EU's approach can be characterized as a "unilateral" approach.[55]

[54] Traditionally, investigating authorities have relied on the Mutual Legal Assistance Treaties (MLATs) to obtain evidences located outside of the territory of their country, bur the process under MLATS is very slow, generally requiring an average of approximately 10 months to complete. President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World" (Dec. 12, 2023) <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed Dec. 13, 2024, p. 227.

[55] The EU's approach can also be characterized as a "regional" approach because it establishes a uniform legal system within the EU.

TABLE 6 Systems for orders to disclose or produce data

	Order to disclose or produce data located outside of the territory	System for resolving conflicts of law	Mechanism to enforce the order against entities outside of the jurisdiction
US CLOUD Act	• Clarifies that US authority can order disclosure of data stored outside of the US (CLOUD Act Sec.103(a)(1), 18 U.S.C. Sec. 2713).	• Establishes a system of motions to quash or modify in the case where the order conflicts with the law of foreign country which concluded an executive agreement with the US (CLOUD Act Sec.103(b), 18 U.S.C. Sec. 2703(h))	• Establish a system of executive agreements, under which authorities can directly order providers of the other party to disclose data (c.f. UK-US Executive Agreement, US-AU Executive Agreement)
EU e-Evidence Regulation/Directive	• Establishes the system of European Production Order that allows an authority of a Member State to order to produce electronic evidence regardless the location of the data (e-Evidence Regulation Art. 1, para. 1).	• Establishes a review procedure in the event of conflicting obligations (e-Evidence Regulation Art. 17).	• Requires Member States to ensure that service providers that are not established in the EU appoint one or more legal representatives in the EU (e-Evidence Regulation Art. 3, para. 1(b)).

Source: Authors' compilation

In addition, the Convention on Cybercrime,[56] signed by the members of the Council of Europe and its observer states (including Japan), addresses the issue of government access to data with a multinational approach.[57] In 2021, 22 parties signed the Second Additional Protocol to the Cybercrime Convention,[58] which includes new provisions for direct cooperation between an authority of one of the party states and private entities of another of the party states.[59]

As recognized in the OECD Government Access Declaration, government access to privately held data is essential for all countries. In order to promote the free flow of data while ensuring effective government access to data, the authors consider that it is important to combine different legal frameworks, in particular: (i) domestic legal systems that eliminate barriers to the free flow of data (e.g. the mutual adequacy arrangement between Japan and the EU), (ii) trade agreements including commitments to eliminate such barriers (e.g. CPTPP Articles 14.11 and 14.13 or Japan-EU EPA new Article 8.81); and (iii) international arrangements for effective data access that promote effective law enforcement while resolving the problem of jurisdictional limitations and conflict of

[56] Convention on Cybercrime (Budapest, 2001).
[57] Convention on Cybercrime, Articles 18 and 32.
[58] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (Strasbourg, 2022) (Second Additional Protocol to the Convention on Cybercrime).
[59] Second Additional Protocol to the Convention on Cybercrime, Articles 6 and 7.

laws (e.g. the executive agreement between the US and the UK).[60] It is also important that these frameworks reflect or incorporate the basic principles set out in the OECD Government Access Declaration to ensure that government access under these frameworks is legitimate. [61]

VI. Conclusion

In the era of 21st century trade, trade rules need to cover issues that were not traditionally considered as trade barriers. The free flow of data is one such issue, and there has been significant development in this area in many RTAs. However, the free flow of data is much more than a trade issue. It requires a careful balance between the economic benefits of trade, the rights of individuals, including the protection of personal data and privacy, and the law enforcement and national security concerns of countries. The DFFT concept provides a forum for reconciling all these different values. There is no "gold standard" on how to balance them, but some fundamental principles such as the rule of law, due process, judicial independence and transparency, as reflected in the OECD Government Access Declaration have the potential to promote cooperation between countries with different regulatory priorities. In that sense, international rulemaking regarding the free flow of data (or more broadly, regarding the digital economy) has the geopolitical potential to strengthen the alliance of countries embracing such fundamental principles.

Kojiro Fujii is a partner at Nishimura & Asahi. He is a member of the Expert Group on Data Free Flow with Trust of the Ministry of Economy, Trade and Industry (METI) of Japan and International Data Governance Expert Group of the Digital Agency of Japan, and the DFFT Experts Community at the OECD. Shunya Muromachi is an associate at Nishimura & Asahi. He is a member of the DFFT Experts Community at the OECD.

---

[60] Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime (Washington D.C., 2019).

[61] Kojiro Fujii and Shunya Muromachi, "Future Directions for Cooperation among Like-minded Countries to Operationalize DFFT with a Focus on Government Access" (2024), RIETI Discussion Paper Series 24-J-018 <https://www.rieti.go.jp/en/publications/summary/24070001.html> (available only in Japanese) accessed Dec. 13, 2024.