The Rules-based Approach to Cope with China: The Case of E-commerce
Fukunari Kimura

Introduction

Japan shares a series of concerns regarding China’s political and economic system with the United States and like-minded countries. Although it is not easy to make China embark on substantial reforms, Japan believes that a rules-based approach could be effective to some extent. One of the focal points is e-commerce or data governance.

There are currently three camps on data governance: the United States and like-minded countries, the European Union (EU), and China. To put it simplistically, the U.S. model uses the free flow of data as a benchmark and allows deviation from the principle as an exception to take care of economic and social concerns. The EU model holds privacy protection as the utmost important value and utilizes extraterritoriality to persuade the rest of the world to be engaged in institutional convergence. The China model serves its own “comprehensive national security” by imposing restrictions on data flows and allowing the government to get access to and inspect data. And now, China is trying to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and challenge the U.S. model.

This is a chance to make Chinese policymakers realize that their political and economic system is incompatible with international rules and norms and encourage reformers in China to initiate drastic reforms. Japan, the United States, and like-minded countries should take advantage of this opportunity to form a majority in international rulemaking for an open, liberal, and dynamic digital world.

Background

Japan and China are geographically close and have had a complicated history. That is why Japan’s approach to China has always been cautious. China has provided a great economic opportunity for Japanese firms, initially as a production site and then as a market. Yet, the political relationship has been fragile. Up to some point, both countries understood the importance of the separation of political issues and economic matters. Although the importance of China as a trade and investment partner has increased, Japanese firms have been careful not to depend on China too much and to separate value chains into a Chinese cycle and a Southeast Asia cycle by applying the “China plus one” strategy. However, this balance was shaken as China started to recognize itself as one of the global superpowers. The Senkaku Island issue in 2010 was a symbolic turning

---

1 Professor, Faculty of Economics, Keio University, Tokyo, Japan and Chief Economist, Economic Research Institute for ASEAN and East Asia (ERIA), Jakarta, Indonesia.
point when China restricted exports of rare earth metals to Japan. Japan quietly started a decoupling of industries with sensitive technologies and rare earths. While South Korea boldly increased its dependency on China in the 2010s, Japan weakened its relative involvement over time.

Japan shares most of the concerns that the United States has regarding China’s political and economic system. However, Japan is not a superpower and thus cannot utilize offensive “economic statecraft.” Instead, Japan has continuously subscribed to the rules-based approach and believes in the power of rules. Since the days of U.S.-Japan trade friction in the 1990s, the Trade Policy Bureau of the Ministry of International Trade and Industry (MITI; currently the Ministry of Economy, Trade, and Industry (METI)) has annually published “The Report on Compliance by Major Trading Partners with Trade Agreements” and has advocated for the importance of the rules-based trading regime under the World Trade Organization (WTO) and bilateral/regional trade and investment agreements. The Japanese Government has almost always been disciplined in conforming with WTO policy measures as a middle power. For Japan, much of the Trans-Pacific Partnership Agreement (TPP) was a solid benchmark of the rules-based trading regime in the Asia-Pacific, and thus it took initiative, together with like-minded countries, to maintain the agreement despite U.S. withdrawal. While the rules-based approach is not perfect for achieving all objectives and cannot control everything in lieu of economic statecraft, it is at least partially effective particularly to cope with China.

Some people may not believe it, but China does care about international rules. It does not mean that China thinks much of the importance of rules and obeys them. Rather, China has a strong desire to be recognized as a respectable superpower by establishing its secure position in international fora. As Watanabe, Kamo, Kawashima, and Kawase (2021) rightly discuss, China’s ambition to gain “institutional discourse power” is pursued through the systematic construction of domestic laws and regulations and its deeper involvement in international rules. China has moved strategically in the past five years by taking advantage of the reduced U.S. commitment under the Trump Administration to multilateral and regional fora, and has tried hard to expand its presence in various international organizations and regional trade agreements. By using its economic influence, China is not shy in obtaining exceptions and exemptions from obligations and even modifying international rules to accommodate China.

---

2 The recent argument on “economic security" in Japan is along a new trend of seeking the possibility of preparing tools for economic statecraft, but I believe that most of the identified items are likely to be limited to defensive ones with proper justification in the rules-based trading regime.

3 I have been a chair of the Sub-committee for the Report since 2016.

4 Remember that Japan did not take any counter measures against the application of Section 232 of the 1962 Trade Expansion Act by the United States while many other countries responded with seemingly WTO non-conforming measures.

The Regional Comprehensive Economic Partnership Agreement (RCEP), which came into effect in January 2022, was China’s starting point for trade rules. During the RCEP negotiations, Japan and Australia worked hard to expand the scope of international rules. In terms of the agenda items, RCEP covers almost all of the policy areas of the CPTPP, except state-owned enterprises (SOEs), labor, and the environment. However, many commitments are not substantive and often explicitly exclude the possibility of dispute settlement. From the viewpoint of China, these negotiations were a practice round of clearing international qualifications, and it sat comfortably in the regional gathering. As a next step, China formally requested its accession to the CPTPP on September 16, 2021, and embarked on a series of external challenges.

E-commerce is one of the front-line agenda items for China’s engagement in international rules. China vigorously set up a series of domestic laws on data and openly advocates for the appropriateness of its regulatory system for cyberspace. Japan, Australia, and Singapore are co-conveners of the WTO Joint Statement Initiative (JSI) on e-commerce, which China also participates in and watches quietly to identify the common denominator of digital rules at the multilateral level. China endorsed the e-commerce chapter of RCEP, which includes two out of the three TPP principles on e-commerce, discussed later in the paper. China seems to be confident about its bid to join CPTPP with its RCEP e-commerce chapter. How effective could the rules-based approach be in dealing with China?

**Key Issues**

1. **China’s Application for CPTPP**

Policymakers in China may assume that their current domestic reforms will allow China mostly to meet CPTPP policy disciplines and that the rest will be resolved through negotiations. Some political leaders from CPTPP member economies quickly gave informal welcoming remarks for China’s application. China seems to be confident in its negotiating power to convince the majority of the CPTPP member economies to accept its application based on its large economic influence.

However, China will face three serious challenges in its accession trial. First, the accession procedure is tough for new entrants. An applying economy must obtain a favorable decision from all existing members twice in the accession process: once at the beginning of the accession process and a second time before joining the group.

---


7 China also submitted an official application for the Digital Economy Partnership Agreement (DEPA) on November 1, 2021. DEPA entered into force on November 23rd, 2021, and the current members are Chile, New Zealand, and Singapore. South Korea also applied for DEPA on September 13th, 2021.
by the TPP Commission and again with the TPP Commission’s final approval for the accession. In the case of the United Kingdom, it took four months, from February 1 to June 2, 2021, to begin the accession process after its formal application. For China, nothing has happened so far since its formal request for accession in September 2021, which indicates that pre-negotiation talks with individual members have not gone well. It seems that China has not convinced all existing members of its readiness. Furthermore, the accession procedure explicitly states that new entrants must “demonstrate the means by which they will comply with all of the existing rules contained in the CPTPP.” This means that a new entrant may not obtain the same level of exceptions or exemptions as the existing members received. This is the same as the WTO accession process; a sort of double standard between existing members and a new entrant could apply. A new entrant might even need to accept some extra commitments and specific monitoring mechanisms as China did in the case of its WTO accession.

Second, the veto given to all existing members means that each individual member’s concerns on the applicant’s trade policy must be properly addressed. Many members have already expressed issues and problems related to China. For example, Japan has listed concerns regarding China’s trade-related policies in its annual report. Australia is suffering from a series of seemingly unjustifiable trade policies by China after it proposed a transparent international investigation on the origin of Covid-19. In addition, to conclude a free trade agreement with a non-market economy, Canada and Mexico may need to obtain the endorsement of the United States, based on the United States-Canada-Mexico Agreement (USMCA) obligation. The clearance of these issues may not be easy even if China attempts to persuade members using its economic power.

Third, China will face many difficulties in fulfilling the CPTPP obligations. The SOEs chapter will certainly be an issue, even though China has recently engaged in SOE reform to enhance the commercial characteristics of SOEs. There is no guarantee that China could obtain the same level of exemptions that Vietnam, Malaysia, and Singapore were allowed. Clearance of the CPTPP labor chapter may be even tougher. China has not achieved a series of obligations posed by the International Labour Organization (ILO) Declaration, which includes freedom of association, the right to collective bargaining, and the elimination of all forms of forced or compulsory labor. China may also have challenges complying with liberalization commitments, which include a high level of liberalization in goods, services, and investment as well as government procurement.

Regarding e-commerce, looking at the issue objectively, China’s reforms are not enough to achieve the requirements for CPTPP accession. To keep the quality of the agreement, CPTPP

---

members should not offer China an easy entry at this moment but should make Chinese leaders realize that their political and economic system is still incompatible with international rules. All CPTPP members have a close economic relationship with China and thus would like to keep the accession talk technical, rather than politicize the issue and face a possible backlash. To maintain such a stance, it is important to clearly identify the inconsistency of the Chinese system with the rules and critically check the quality of Chinese proposals.

2. Three TPP Principles on E-commerce

The TPP e-commerce chapter became the e-commerce chapter in CPTPP without any modification. Newer agreements concluded by the United States such as the USMCA and the U.S.-Japan Digital Trade Agreement include some updates in e-commerce contents, but the basic structure of the chapter is the same.

Chapter 14 of TPP contains several relatively innocuous items such as no imposition of customs duties on electronic transmissions, non-discriminatory treatment of digital products, electronic authentication and electronic signatures, online consumer protection, personal information protection, and others. More importantly, the “three TPP principles” on e-commerce are highlighted: cross-border free flow of data (Article 14.11), no data localization requirement (Article 14.13), and prohibition of forced disclosure of source code of software (Article 14.17).

The third one, the source code issue, clearly reflects concerns on data-related regulations in China. Article 14.17 says, “No party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory,” excluding software used for critical infrastructure. This will surely be one of the obstacles for China to come into the CPTPP.

Regarding the first two principles, Chinese leaders perhaps think that they can clear these requirements by receiving exceptions.

Both Article 14.11 and Article 14.13 start with a note that a member “may have its own regulatory requirements,” which reflects the TPP philosophy that the complete convergence of regulatory frameworks is not expected. However, because of that, it is important to check whether basic principles are fulfilled or not.

Article 14.11 states “Each party shall 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.” And members can adopt or maintain measures “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.” Article 14.13 states, “no party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in the territory.” And the same “legitimate public policy” exception follows. This is a similar approach to General Agreement on Tariffs and Trade (GATT) Article 20 General Exceptions where economic efficiency and other values, in this case public policy, should reconcile with each other. The boundary of exceptions is not clear from the text.

In addition, overarching security exceptions are given in Article 29.2 of the CPTPP, which says, “Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.” This looks parallel to GATT Article 21 Security Exceptions where many scholars claim that national security should be based on self-judgment.

How these two kinds of exceptions, based on legitimate public policy and security considerations, are granted is crucial.

3. China’s Domestic Laws and Regulations

In the past five years, China has been keen to establish a comprehensive data-related regulatory framework. While numerous laws and regulations have been announced, three major domestic laws have recently come into effect: the Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information Protection Law (2021). These laws were introduced due to national security concerns and include data access and safety inspections by the government, data localization requirements, and restrictions on the free flow of data, in addition to possible discriminatory treatments against foreign businesses that may be inconsistent with the multilateral commitments under the General Agreement on Trade in Services (GATS). While the Personal Information Protection Law takes care of personal data only, the Cybersecurity Law also covers “important” data, and the Data Security Law controls all sorts of data. The basic philosophy of these laws is the exact opposite of the U.S. model, and the issue is whether they can be legally consistent with “free flow of data” and “no data localization requirement” of the CPTPP if using the social policy exception or national security exemption. The concept of social policy and national security in China is different from the Western world, and Japan and the United States must be ready to point out the inconsistency in legal terms.

RCEP includes two principles out of the three aforementioned principles on e-commerce: free flow of data and no data localization requirement. Japan and Australia strongly pushed for their inclusion during the negotiations. China accepted this under the condition that the chapter explicitly states that a member can define its own security exceptions and that it is excluded from
dispute settlement, which means that China would have a free hand in the usage of security exceptions.\textsuperscript{11}

4. Principles and Exceptions

The TPP e-commerce chapter advocates free flow of data and no data localization requirement as principles. Setting the economically efficient laissez-faire equilibrium as a benchmark is the right approach based on standard public economics aimed at aligning policies to mitigate market failures and reconcile economic efficiency with other values.\textsuperscript{12} And just calling for the principles is not enough; policies that possibly go against these principles must be carefully assessed. However, such policy evaluations have not been conducted yet.

Recently, many countries have introduced various restrictions on the flow of data as well as data localization requirements. Cory and Dascoli (2021) present a list of data localization requirements introduced by many countries in the world and discuss multiple rationales used for justifying the introduction of such measures.\textsuperscript{13} Sheppard, Yayboke, and Ramos (2021) present various forms of data localization requirements and varying rationales as well as their national security implications.\textsuperscript{14} Privacy protection is one of the popular reasons, perhaps stimulated by the EU General Data Protection Regulation (GDPR), though the scope of personal data to be protected and measures for protection differ across countries. National security concerns are another typical excuse, particularly with the increase in geopolitical tensions and the threat of cyberattacks. In both cases, the necessity of data localization for data protection is not often clear. Other countries

\textsuperscript{11} DEPA also includes cross-border free flow of data (Article 4.3) and no data localization requirement (Article 4.4) with exceptions for legitimate public policy purposes as well as security exceptions (Article 15.2), which basically duplicates TPP. However, as RCEP poses, these commitments are explicitly excluded from dispute settlement (Article 14A.1). Furthermore, Annex I reaffirms that Articles 4.3 and 4.4 “do not create any rights or obligations between or among the Parties under this Agreement.” Although DEPA includes some novel business-friendly issues such as artificial intelligence and fintech as good references for a future agreement, it does not fully step into the core issues of digital governance.


advocate different reasons including data protectionism. Careful reviews are required for evaluating the appropriateness of these measures.

CPTPP intends to build up the basis of data-related policy disciplines in the Asia-Pacific and thus must clarify the boundary of social policy and national security exceptions. This mission has not yet been completed. The problem partially comes from the inactive monitoring function in the CPTPP. Once an agreement is in effect, members must conduct a peer review or surveillance to check how the series of commitments are fulfilled. In the case of the e-commerce chapter, the TPP Commission must take the initiative for conducting reviews on how related domestic laws and regulations in each country are revised and implemented. By doing so, the commission could accumulate cases to indicate the boundary of exceptions. This is one of the tasks that CPTPP members must work toward. CPTPP members should admit their weakness in self-discipline after the United States, a strong rule observer, walked away from the agreement.

In addition, Japan, the United States, and like-minded countries should get together to establish a system of international rules on data-related policies beyond CPTPP, the U.S.-Japan Digital Trade Agreement, and other agreements.

Policy Recommendations

Here are four policy recommendations for Japan, the United States, and like-minded countries in the Asia-Pacific.

1. Utilize the rules-based approach effectively to cope with China

China’s political and economic system is a serious concern for Japan, the United States, and like-minded countries. The rules-based approach can be an effective tool for conveying this concern to Chinese policymakers.

As mentioned above, China does care about international rules—not because it appreciates rules itself but because it would like to gain “institutional discourse power” and be a respected superpower in international fora. The rules-based approach may not be enough for China to initiate substantial reform. However, it may at least make Chinese leaders recognize the incompatibility of their political and economic system with international rules and encourage reformers in China to call for further reform.

Digital rules and norms are on the front-line of agenda items for which the rules-based approach could be effective. Japan, the United States, and like-minded countries must be strategic to push forward in this direction.
2. Strengthen the monitoring function in CPTPP

The CPTPP entered into effect in December 2018 with Mexico, Japan, Singapore, New Zealand, Canada, and Australia, followed by Vietnam in January 2019 and Peru in September 2021. However, it seems that CPTPP members have not yet conducted rigorous monitoring of the implementation of CPTPP commitments.

The CPTPP poses three TPP e-commerce principles: cross-border free flow of data, no data localization requirement, and prohibition of forced disclosure of source code of software. Particularly regarding the first two principles, it is important to clarify the boundary of public policy and security exceptions by accumulating cases through peer monitoring. Data-related laws and regulations, as well as their implementation, must be reviewed by the TPP Commission, and it should point out inconsistencies if necessary.

In the case of Vietnam, Article 14.18 states that its consistency with the former two principles and others would not be subject to dispute settlement for two years after the agreement comes into effect. Two years have already passed, and thus a peer review must be conducted. Vietnam’s Cybersecurity Law has common elements with China’s law, particularly for data localization requirements, and may need some revision to be consistent with CPTPP obligations. In addition, the accession negotiation for the UK is ongoing. This case would also provide useful information on how to allow or not to allow exceptions.

By accumulating cases, CPTPP members must be ready to specifically point out the inconsistency of the Chinese legal structure with the three TPP principles.

3. Sharpen the conceptual argument against China’s data-related policies

The China model on data-related policies is extremely inward-looking and thus cannot be an international model. Japan, the United States, and like-minded countries should pursue an open and outward-looking framework. To do so, these countries should sharpen their logic to point out problems with China’s data-related policies.

Detailed legal advice, as well as practical comments from the private sector, should be considered regarding the following three recommendations. First, there should be a clear distinction between personal data and non-personal data. Each country has a different definition of personal data, different scope of personal data to be protected, and different ways to protect personal data (e.g., whether data localization is necessary or not). There must be some flexibility to cope with each country’s judgment on personal data. On the other hand, non-personal data or
data in private economic activities must be basically allowed to flow freely, domestic and cross-border.\textsuperscript{15} This could be one of the counterarguments against the Chinese system on data.

Second, some sort of “code of conduct” in accessing private data by the government could be explicitly introduced. In the physical world, democratic countries typically have some specific legal procedure for the government to step into a private entity, even in the case of criminal investigation. However, in cyberspace, it is unclear if this discipline should be imposed on the government. Although the ultimate resort is people’s trust in each country’s government, whether some discipline can be imposed or not is one of the crucial points in setting up international rules. Even in cases where ex-ante restriction on the government’s conduct is difficult, ex-post traceability and room for court challenge could be secured.\textsuperscript{16}

Third, Japan and the United States must define the boundary of national security exceptions more clearly. Since 2014, China has applied the concept of “comprehensive national security,” which is a much more widely defined security concept than what the Western world typically subscribes, including political security, technological competitiveness, and others. Is it possible to legally negate such a widely defined national security concept as a basis for exceptions? The best way to do so, though it may be difficult, is to directly highlight the difference between “comprehensive national security” and the concept of national security in the Western world and to apply national security exceptions only for the latter. Even if the concept of national security itself is not questioned, there should still be review of the necessity of the policy measure and whether it is applied in a discriminatory manner, drawing on similarities from GATT Article 20. The issue is that GATT Article 21 has been interpreted as providing room for self-judgment on national security exceptions. That is why countries have been cautious and mostly self-restrained about the usage of GATT Article 21. However, in the case of digital governance, this is a core issue. How clearly the boundary of exceptions can be set is a very important challenge.

4. Start working for a U.S.-led new digital agreement in the Asia-Pacific

The TPP principles, which include free flow of data and no data localization requirement as benchmarks, are the proper approach to develop an open, liberal, and dynamic digital economy and can be a model for many countries, different from the EU model or the Chinese model. The United States, Japan, and like-minded countries can develop a new digital agreement centered on

\textsuperscript{15} Although the definition of personal/non-personal data is arguable, the EU clearly supports the free flow of non-personal data as a principle.

\textsuperscript{16} Japan pointed out a potential problem of unlimited government access to data at the occasion of reviewing OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data in November 2019, and the Committee on Digital Economy Policy (CDEP) in the OECD acknowledged a concern on the absence of common rules for government data access in December 2020. The G7 Trade Ministers in October 2021 announced the G7 Trade Ministers’ Digital Trade Principles (Annex B) that advocated “(a)chieving consensus on common principles for trusted government access to personal data held by the private sector will help to provide transparency and legal certainty” (https://www.meti.go.jp/press/2021/10/20211022008/20211022008-3.pdf).
these principles, including more specific rules regarding exceptions for public policy and national security, as well as on the government’s access to data.

In the same spirit, Japan proposed the concept of “data free flow with trust (DFFT)” in the G20 in 2019. Although the word became popular in policy discussions, this concept has not been substantially developed since then, perhaps because Japan does not have enough resources to devise a legal system for data governance. Although the JSI on e-commerce in the WTO is an example of meaningful engagement, it is unlikely to establish a full-fledged framework with workable policy disciplines for free flow of data and no data localization requirements with well-defined exceptions. Under the leadership of the United States, Japan and others can establish a solid basis of data governance.

Many countries including ASEAN member states also feel uncomfortable accepting China’s data policy. China monopolizes domestic data based on its wide definition of national security while collecting data abroad for its businesses. A “great digital firewall” may soon be inevitable. Japan, the United States, and like-minded countries must form a majority by increasing subscribers to the U.S. model. It would be great if CPTPP members could be included with priority; East Asia has been waiting for a U.S. comeback for many years. In addition, if a new agreement could include the whole of ASEAN, the framework would become particularly effective for making China realize its problems.

It would certainly be desirable to connect a new digital agreement with the Indo-Pacific Economic Framework. However, at this moment, Japan and the United States cannot be very optimistic. India is also constructing a peculiar policy environment on data issues in its own way. Japan and the United States should not degrade the quality of a new agreement because of India.

**Conclusion**

The United States has been the most powerful rule maker and rule observer in the world. It is natural for the United States to establish global rules for data-related policies as the most digitally advanced country. It is also important for the United States to set the benchmark for the free flow of data and layout policies to countervail market failures and reconcile other values such as privacy protection and national security.

The CPTPP is a vehicle that Japan has maintained for the United States to accomplish this. Unfortunately, the United States is unlikely to come back to TPP due to political reasons. However, the United States can still utilize this vehicle, with cooperation from Japan and other allies and partners that are members, to disseminate U.S. ideas to the Asia-Pacific region including countries at different development stages and with different political regimes. Particularly on digital rules, China is inward-looking, and this is a chance to form a majority in rulemaking.
Again, China does care about international rules to be recognized as a respectable superpower. Although the Russo-Ukrainian War will generate multiple global repercussions, one thing for sure is that China is likely to become more aware of the risk of economic isolation due to possible economic sanctions and strengthen its effort to gain “institutional discourse power.” We must take advantage of this fact and make Chinese leaders realize that their political and economic systems are not compatible with international rules. This strategy can be applied not only for digital rules but also other topics such as SOEs, subsidies, labor, and intellectual property protection. The cost of implementing the rules-based approach is low, probably much lower than imposing tariffs or implementing extensive decoupling, let alone hard-core national security operations. Japan and the United States should effectively employ soft power to establish a rules-based approach to digital governance.