YUKO SUDA

Japan's Personal Information Protection Policy Under Pressure

The Japan-EU Data Transfer Dialogue and Beyond

ABSTRACT

This article explores the politics surrounding the recent data transfer agreement between Japan and the European Union, with a focus on the linkage between Japanese domestic politics and foreign pressure on Japan's personal information protection policy. The agreement may be seen as one of mutual recognition, in that Japan and the EU mutually recognized the other as providing an "adequate level of protection" for personal data. However, a close examination of the case suggests that Japan made substantial efforts to meet the EU's standards for adequacy in order to enhance the interests of transnationalized Japanese firms that rely on the flow of personal information across borders. In sum, the latest changes in Japanese personal information protection regulation paved the way for the Japan-EU data transfer agreement; these changes were precipitated by the extraterritorial effect of the EU's data protection laws, which had resonated within Japan's domestic politics.

KEYWORDS: Japan-EU relations, privacy, data transfer, foreign pressure, regulatory politics

INTRODUCTION

Today, with the rise of the digital economy and globalization, a vast amount of data flows across borders, primarily for purposes related to transnational economic activities. According to one study, cross-border data flows grew

YUKO SUDA is an Adjunct Lecturer at Tokyo University of Foreign Studies. She is the author of *The Politics of Data Transfer: Transatlantic Conflict and Cooperation over Data Privacy* (Routledge, 2017). The author is grateful to Yuichi Morii and the anonymous reviewer for their helpful comments. Part of this research was funded by a research grant from the Telecommunications Advancement Foundation. Email: <ysuda@tufs.ac.jp>.

Asian Survey, Vol. 60, Number 3, pp. 510–533. ISSN 0004-4687, electronic ISSN 1533-838X. DOI: https://doi.org/10.1525/AS.2020.60.3.510.

45 times between 2005 and 2014 (McKinsey Global Institute 2016). While the value of transborder flows of data has been recognized since the 1970s, such recognition is likely to be further enhanced by the diffusion of new technologies such as cloud computing and big-data analyses.

At the same time, there is widespread recognition, at least in democratic countries, that data containing personal information (e.g., names, addresses, and telephone numbers) should be protected (Reidenberg 2000). In fact, virtually all democratic states have some form of privacy or data protection laws, which define, in one way or another, the limits on the processing and use of personal information or data (Bennett and Raab 2006). However, since data that flow across borders include personal data, the regulation of their transfer to a foreign jurisdiction might inhibit, if not disrupt, international data transactions.

Like other governments of advanced industrialized democracies, the Japanese government is aware of the need to reconcile the potentially conflicting objectives of the free flow of data across borders and the protection of personal data. In the words of the "Basic Policy on the Protection of Personal Information," which the cabinet finalized in April 2004 and then revised in June 2018, "as the cross-border flow of data containing personal information is increasing, it is required to ensure internationally that data can flow smoothly [across borders] while also protecting personal information."[1]

Recently, Japan and the EU have agreed to "create the world's largest area of safe data transfers based on a high level of protection of personal data" (European Commission 2018a; PPC 2018b) through a framework of mutual adequacy decisions. The Japan-EU data transfer agreement, which was reached in July 2018 following two years of dialogue and took effect in January 2019, can be seen as one of mutual recognition and a kind of regulatory cooperation, in that the governments of Japan and the EU mutually recognized the other as providing an "adequate level of protection" of personal data. However, a close examination of the case suggests that Japan made substantial efforts to meet the EU standards for adequacy. In fact, Japan amended its personal information protection act prior to the dialogue, in part to attain "international harmonization."

1. "Kojin Joho no Hogo ni Kansuru Kihon Hoshin" [Basic Policy on the Protection of Personal Information], <https://www.ppc.go.jp/files/pdf/300612_personal_basicpolicy.pdf>, accessed March 30, 2019.

Such an account might create a sense of déjà vu for students of Japanese foreign economic policy. It has been argued that Japan tends to react to outside pressure for change, especially pressure from its principal trading partner and security ally, the US. Do the latest changes in Japanese personal information protection regulation represent yet another example of Japan's responsiveness to foreign pressure——in this case, to pressure from the EU, a leading writer of global regulatory rules?

This article explores the politics surrounding the Japan-EU data transfer agreement with a focus on the linkage between Japanese domestic politics and foreign pressure on Japan's personal information protection policy. Although recent developments in this policy seem to be largely consistent with the interpretation that Japan is a "reactive state," in which "the impetus to policy change is typically supplied by outside pressure" (Calder 1988, 518), much remains to be examined about the domestic regulatory politics of Japan, the regulatory influence of the EU, and, above all, their interplay. Indeed, one important insight that may be gained from the study of *gaiatsu* ("foreign pressure") is that *gaiatsu* is likely to yield an intended response from Japan when it positively "reverberates within Japanese domestic politics" (Schoppa 1997, 4).

In the following sections, I will first present a brief review of the evolution of the Japanese personal information protection regime to show how Japan's data privacy regulation came to converge with European data protection rules. I will then examine the Japan-EU data dialogue and analyze the case from three viewpoints: (1) the bilateral economic relationship between Japan and the EU; (2) the international interests of major domestic actors in Japan, that is, transnationalized Japanese firms that rely on the flow of personal information across borders; and (3) the extraterritorial or beyond-the-border effect of the EU's data protection laws, which has resonated within Japan's domestic politics and thereby allowing the EU to exert regulatory influence on Japan in this crucial policy area. I will conclude the article with discussion on the implications of the analysis findings.

JAPAN'S PERSONAL INFORMATION PROTECTION REGIME

Over the past 30 years, Japan has gradually institutionalized the protection of personal information, forming a trajectory that is rather different from that of Western European countries or the EU.

The Act on the Protection of Personal Information Held by Administrative Organs

In 1988, the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO), "the first law that specifically dealt with privacy in Japan" (Kawabata 2016, 264), was enacted, partly in response to the adoption of the Privacy Guidelines by the Organization for Economic Co-operation and Development (OECD) in 1980. The legislation was a remarkable step in the development of the Japanese privacy regime. However, the APPIHAO was designed to regulate the handling of digitalized personal information by government organizations. For the private sector, there only were legally non-binding guidelines issued by competent authorities.

This means that Japan's approach to personal information protection was different from the European approach to data protection. In Europe, data protection laws generally cover both the public and private sectors, such that "data controllers" are legally regulated without a sectoral distinction. Significantly, the 1995 Data Protection Directive, the cornerstone of the EU data protection regime, did not distinguish between the public and private sectors in its application.

Such a difference could matter greatly if private entities (e.g., firms) in Japan were to receive personal data from the jurisdiction of the EU. The Data Protection Directive allowed the transfer of personal data from EU Member States to a third (i.e., non-EU) country only if the third country in question ensured an "adequate level of protection" (Article 25). This provision "had clear external consequences" (Farrell 2003, 285) because, in principle, it prohibited the export of EU citizens' personal data to third countries that did not have "adequate" protections for individual privacy in place.

The problem for Japan was that an assessment of adequacy under the Data Protection Directive was based on, among other things, "the rules of law" in force in the third country in question. To be considered as ensuring an "adequate level" of protection, the third country needed to have an omnibus data privacy legislation, not a sectoral one like the APPIHAO. In fact, while the pressure of the Data Protection Directive on non-EU countries resulted in the spread of European-type privacy laws, Japan was one of the few OECD countries that "failed" to enact a comprehensive privacy law (Bennett 1998).

The Enactment of the Act on the Protection of Personal Information

The next milestone in the evolution of the Japanese privacy regime was the enactment of the Act on the Protection of Personal Information (APPI) in May 2003. With the aim to "protect an individual's rights and interests while considering the utility of personal information" (Article 1), the APPI sets forth obligations for "personal information handling business operators," which include the specification of the purpose for using personal information, limitations on the use of personal information to achieve the specified purpose, the proper acquisition of personal information, notification of the purpose of use at the time of acquisition, and the assurance of data quality. These obligations correspond to the purposes, the use limitation, the collection limitation, and the data quality principles of the OECD Privacy Guidelines, respectively.

It is worth noting that the APPI was passed in conjunction with the controversial Basic Resident Registers Network (*Juki*-net) project. *Juki*-net is a nationwide computer network composed of the resident databases of municipal governments. Since *Juki*-net allows administrative organizations to share residents' personal information stored in the databases, the plan and eventual introduction of the network in August 2002 raised grave privacy concerns. Therefore, the policy process that led to the passage of the APPI was arguably accelerated by *domestic* debate over the use of personal information in a networked environment.

However, *international* considerations did play a role in the legislation of the APPI. As with the APPIHAO, the APPI was drawn up with reference to the OECD Privacy Guidelines, and was therefore in line with an internationally agreed-upon set of privacy principles. However, this was not entirely the case with the European data protection standards.

Although the APPI brought the private sector within the purview of legal regulation,[2] there were at least three major discrepancies between the Japanese personal information protection regime and the EU data protection regime. First, while the application of European data protection laws was overseen by independent authorities called the Data Protection Authorities (DPAs), such a third-party authority was absent in Japan. This absence

2. However, businesses that held the personal information of fewer than 5,000 individuals were exempted from the obligations of the APPI. This exemption was revoked when the APPI was amended in 2015.

apparently constituted a serious institutional flaw for the Europeans, who believed that data protection was a matter of social protection and should be guaranteed by public authorities (Kobrin 2004).

Second, while the Data Protection Directive prohibited the processing of "special categories of data," defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life" (Article 8), the APPI did not have a provision on sensitive information.

Third, while the EU Directive provided rules on the transfer of data to a third country, the APPI was silent on the cross-border transfer of personal information. Therefore, technically, personal data transferred from the EU to Japan could be further transferred to another country that did not ensure an "adequate level" of protection.

The Amendment of the Act on the Protection of Personal Information

The APPI was amended in September 2015 pursuant to the blueprint laid out in the "Policy Outline of the Institutional Revision for Utilization of Personal Data," which the Japanese government's Information Technology (IT) Strategic Headquarters had finalized in June 2014. According to the "Policy Outline," the main purpose of the revision was the reduction of "a barrier to the utilization personal data" to revitalize Japanese industries and thereby promote the growth of the Japanese economy (IT Strategic Headquarters 2004, 6–7).

The centerpiece of the amendment was the inclusion of provisions on "anonymously processed information," that is, information relating to an individual that has been irreversibly processed as personally unidentifiable. The new provisions were a response to the frustration of Japanese businesses, which were eager to use personal information more extensively to reap the full benefit of technological innovation. In particular, the amended APPI was expected to facilitate the use of big data in the form of "anonymously processed information."

At the same time, the amended APPI provides strengthened safeguards for individuals' right to data privacy. First, business operators handling personal information are now prohibited from acquiring "special care-required personal information," defined as personal information concerning an individual's "race, creed, social status, medical history, criminal record, fact

of having suffered damage by a crime" without obtaining the individual's consent in advance (Article 17).

Second, the amended APPI sets conditions under which personal information can be transferred to a third party in a foreign country. Specifically, it provides that business operators must obtain advance consent from the individual whose personal data are to be sent to a third party located outside of the territory of Japan *except for* the case in which the foreign country in question has a "personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests" (Article 24).

Third and most importantly, the amended APPI contains provisions on an independent third-party agency named the Personal Information Protection Commission (PPC), granting it the authority to give guidance, advice, recommendations, or an order to personal information-handling business operators (Articles 41 and 42). These provisions led to the establishment of the PPC in January 2016, which, according to Masao Horibe, the PPC's first chairperson, constituted "a significant step forward harmonizing Japanese data protection framework with international one" (PPC n.d.a).

Meanwhile, in the EU, a sweeping overhaul of the data protection regime was underway. The reform process began in December 2009, when the Council of the EU, the EU's essential decisionmaker, invited the European Commission, the executive arm of the EU, to "evaluate the functioning of the various instruments on data protection and present, where necessary, further legislative and non-legislative initiatives" (Council of the EU 2009, 2.5). In response, the European Commission submitted a proposal in January 2012 for the General Data Protection Regulation (GDPR), which would replace the Data Protection Directive (European Commission 2012). The GDPR was adopted by the European Parliament and the Council in April 2016.

Like its predecessor, the GDPR has an extraterritorial clause providing that "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection" (Article 45). In other words, the transfer of personal data beyond the EU border may be based on an "adequacy decision," which is made by considering various elements, including "relevant legislation" of the third country in question.

The Shadow of Future Talks with the EU

As a result of the amendment of the APPI, the Japanese personal information protection regime came to have more in common with the EU's personal data protection regime than previously. In fact, the amendment could be seen as one part of the efforts toward "international harmonization," which signified alignment with the data protection rules of the EU, in practice.

The APPI was amended with the recognition that the international landscape of data privacy regulation was changing, as the OECD revised its Privacy Guidelines in July 2012; the Obama administration released the draft of the Consumer Privacy Bill of Rights in February 2012 (White House 2012), and the European Parliament voted in support of the proposal for the GDPR in March 2014 (European Parliament 2014). Taking note of these developments, the IT Strategic Headquarters' "Policy Outline" stated the following:

> With the globalization of corporate activities, the need has arisen for Japanese companies to share or mutually transfer their personal data with foreign companies. To make such sharing and transfer of personal data possible, it is necessary to develop an internationally harmonized, reliable [personal information protection] system [in Japan] . . . (IT Strategic Headquarters 2004, 9).

Presumably, the development of an "internationally harmonized" system denoted foremost harmonization with the EU rules, because Japanese personal information regulation was already in line with the OECD Privacy Guidelines and the US did not have a comprehensive privacy law to emulate in the first place.

Interestingly enough, the Japanese government seemed to assume that the harmonization or resolution of discrepancies with the EU data protection rules was a precondition for negotiations with the EU regarding a framework for the smooth transfer of data. When the bill on amending the APPI was deliberated in the Diet, Yamaguchi Shunichi, Minister in Charge of IT Policy, stated that "we have taken all necessary measures. We would like to actively exchange information with the EU upon the passage of the bill" (Anonymous 2015a). In short, the APPI was revised partly in anticipation of talks with the EU.

THE JAPAN-EU DIALOGUE ON DATA TRANSFER

The Japan-EU dialogue on the transfer of personal data was an attempt to enhance the EU's understanding of the *amended* APPI and the Japanese understanding of the GDPR. However, in actuality, the dialogue revolved around the question of Japan's adequacy.

A Decent Start

In April 2016, the newly established PPC and the European Commission's Directorate-General for Justice and Consumers had their first dialogue on data privacy regulation. The Japan-EU dialogue continued into 2017 with a view toward building a framework for the "mutual and smooth transfer" of personal data between Japan and the EU.[3]

Japan was not the first country with which the EU worked to develop a framework for data transfer. However, few jurisdictions succeeded in obtaining an adequacy decision, because meeting the EU standard was extremely challenging. In fact, Australia attempted to negotiate a data exchange agreement with the EU only to discover that the Australian Privacy Act did not meet the EU's adequacy requirement (Article 29 Data Protection Working Party 2001).

When Japan and the EU began their data transfer dialogue, only 10 jurisdictions had obtained adequacy decisions from the European Commission.[4] Notably, in 2016, the EU reached an accord with the US, the EU's largest trading partner, on the Privacy Shield Framework for the transfer of personal data based on an adequacy decision. However, the Privacy Shield is based on a "partial" adequacy decision, because the US does not have a privacy law to comprehensively regulate information practices in the private sector.[5]

3. The PPC held meetings with its counterparts in other jurisdictions, including European countries, to promote "cooperation with foreign authorities." However, the interactions between Japanese and European privacy officials seems to be far less dense than the interactions between EU and US officials, who formed transnational networks to have their interests reflected in the data protection or sharing policies. For more on transatlantic alliances between privacy and security officials and their impact on EU-US data disputes, see Farrell and Newman (2019).

4. They were Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the United States. The adequacy decision on Canada is also "partial" and is limited to commercial organizations.

5. The US Privacy Act only applies to the public sector, leaving the private sector with a fragmented system of sector-specific legislations and self-regulation.

As for Japan, the European Commission was "a bit more ambitious.[6] In the Communication of January 2017, the European Commission (2017) made it clear that it would prioritize discussions on a possible adequacy decision with Japan, along with other key trading partners in East and Southeast Asia.[7] The PPC, for its part, was positive about designating the EU as a "foreign country" with personal information protection standards equivalent to those of Japan. Thus, in July 2017, the PPC and the European Commission confirmed that, on the basis of "strengthened mutual understanding," they would seek "to further facilitate smooth and mutual data flows, in particular through simultaneous finding of an adequate level of protection by both sides" (PPC 2018a). They hoped that they would find an adequacy of their respective systems by early 2018, that is, before the GDPR came into force on May 25, 2018.

The Japan-EU Data Dialogue and the Japan-EU EPA Negotiations

It is noteworthy that the Japan-EU data dialogue was held almost in parallel with the negotiations for the Economic Partnership Agreement (EPA) between Japan and the EU, which were kick-started in March 2013 (Ministry of Foreign Affairs 2013). The trade negotiations were accompanied by the data transfer dialogue, because the EPA was expected to increase the flow of goods, services, and money, and concomitantly, the exchanges of data between the EPA partners. According to the PPC and the European Commission, "a simultaneous finding of an adequate level of [data] protection by both sides" was thought to "complement and enhance the benefits of" the Japan-EU EPA (PPC 2018a).

However, the Japan-EU data dialogue was *not* a part of the Japan-EU EPA negotiations because the Europeans believe that data protection is a fundamental right and thus non-negotiable.[8] The European Commission insisted that, "The EU data protection rules cannot be the subject of negotiations in a free trade agreement" and that "dialogues on data protection and trade

6. Interview with an official of the European Commission, September 5, 2017.

7. The European Commission also gave priority to South Korea in its assessment regarding which third countries should be pursued for a dialogue on adequacy.

8. The EU Charter of Fundamental Rights (Article 8) states that "Everyone has the right to the protection of personal data concerning him or her."

negotiations with third countries have to follow separate tracks" (European Commission 2017, 9).

Toward a Mutual Adequacy Finding

Throughout 2017, the PPC and the European Commission worked together toward the goal of "simultaneous finding of an adequate level of protection by both sides." In essence, the achievement of this goal hinged on whether the European Commission would recognize that the level of protection in the Japanese system was "essentially equivalent" to that guaranteed in the EU system.[9]

While acknowledging the similarities of the EU and Japanese systems, the European Commission raised several concerns about the level of personal information protection guaranteed by the APPI and the related Cabinet Order (Anonymous 2017a; Anonymous 2017b). Specifically, the European Commission was concerned that, unlike the "special categories of data" in the GDPR, "special care-required personal information" as defined in the APPI did not include information on sexual orientation and trade union membership. In addition, the European Commission was apprehensive about the exception that the APPI and the related Cabinet Order effectively made to an individual's right of access to his or her data. The APPI required personal information handling business operators to disclose "retained personal data" to an individual upon his or her demand, but "retained personal data" as defined in the APPI and the Cabinet Order to Enforce the Act on the Protection of Personal Information No. 507 excluded data that were set to be deleted within six months.

Since the Japanese government was reluctant to further amend the APPI, in late 2017, the PCC floated the idea of guidelines specially made to ensure a "high level of protection" of the personal information transferred from the EU, based on an adequacy decision. In April 2018, the PPC (n.d.b) made the draft guidelines public for comments. The guidelines described the practices with which business operators handling personal information received from the EU should conform, in addition to complying with the obligations under the APPI. Business operators should handle EU-originating data related to an

9. A finding of adequacy "does not require a point-to-point replication of EU rules" but instead a level of protection that is "essentially equivalent" to that guaranteed in the EU (European Commission 2017, 6–7).

individual's sexual activity, sexual orientation, or trade-union membership in the same manner as "special care-required personal information," treat personal data forwarded from the EU as "retained personal data," regardless of the retention period of the data, and delete information related to data anonymization methods from "anonymously processed information" obtained from the EU, such that it would be impossible to re-identify individuals.

Nonetheless, at the prompting of the European Commission, the PPC decided to formulate these additional requirements as binding rules rather than non-binding guidelines, which would supplement the APPI (Anonymous 2018). By May 2018, the PPC and the European Commission had agreed to bridge the "relevant differences between the two systems" through Supplementary Rules (PPC 2018a).[10]

The Mutual Adequacy Arrangement

On July 17 (the day the Japan-EU EPA was signed), Commissioner Kumazawa Haruhi of the PPC and Commissioner Věra Jourová of the European Commission made a joint statement that they had "successfully concluded discussions to recognise each other's personal data protection systems as equivalent" (PPC 2018b). In other words, the PPC and the European Commission reached a final agreement on the establishment of a framework for the "mutual and smooth transfer of data" between Japan and the EU through reciprocal adequacy decisions.

The statement was happily received by the Japanese business community, which had been longing for such a framework for data transfer. As Nakanishi Hiroaki, Chairman of the Japan Business Federation (Keidanren 2018) commented, Japanese businesses "welcome that Japan and the EU have successfully concluded discussions to recognise each other's personal data protection systems as equivalent, through which . . . cross-border personal data flow will be facilitated."

The Japan-EU agreement was subsequently followed by unilateral actions on each side. In Japan, the PPC further proceeded with the procedures under Article 24 of the APPI and, on January 18, 2019, decided to designate the EU as a "foreign country" with personal information protection standards

10. Accordingly, the PPC issued the Supplementary Rules in September 2018. The rules took effect on January 23, 2019.

equivalent to those of Japan (PPC n.d.c).[11] The designation was scheduled to take effect on January 23, 2019.

In the EU on September 5, 2018, the European Commission launched procedures for the adoption of an adequacy decision on Japan (European Commission 2018b). The procedure for an adequacy decision involves a proposal from the European Commission, approval from a committee composed of representatives of EU Member States, and, importantly, an opinion from the European Data Protection Board (EDPB), which replaced the Article 25 Working Party upon the entry into the application of the GDPR.

The EDPB adopted its opinion on the draft adequacy decision on Japan on December 5, 2018. In the opinion, the EDPB (2018) noticed that "a number of concerns" remained regarding the adequacy of the level of protection afforded to individuals in the Japanese framework. For example, the EDPB was concerned with the possible onward transfer of EU-originating personal data to a third country.[12] However, notwithstanding the concerns, the EDPB neither endorsed nor rejected the Commission's draft adequacy decision, opening the way for Japan to become the first Asian country to obtain an adequacy decision.

Another notable development was that, upon the request of the European Commission, on September 14, 2018, Kamikawa Yoko, the Japanese Minister of Justice, sent Commissioner Jourová a document titled "Collection and use of personal information by Japanese public authorities for criminal law enforcement and national security purposes" (Ministry of Justice et al. 2018). In the document, the Japanese government gave "assurances that government access to personal information transferred from the EU to Japan will be limited to what is necessary and proportionate" and would be subject to an independent oversight and redress mechanism.

On January 23, 2019, the European Commission adopted a decision that "Japan ensures an adequate level of protection for personal data transferred from the European Union to personal information handling business operators in Japan subject to the Act on the Protection of Personal Information as

11. To be precise, the PCC designated the European Economic Area (EEA), which includes EU Member States and Iceland, Norway, and Lichtenstein, because the GDPR was incorporated into the EEA Agreement in July 2018.

12. The transfer of personal data from Japan to a third party in a foreign country requires that the foreign country in question has the level of protection equivalent to the one guaranteed by the APPI, not complemented by the Supplementary Rules.

complemented by the Supplementary Rules" (European Commission 2019a, 1.1). With both sides having completed the domestic procedures, the Japan-EU framework for the "mutual and smooth transfer" of personal data came into effect on that date (PPC 2019).

ANALYSIS

The politics surrounding the EU-Japan data transfer dialogue can be analyzed from different points of view, each of which highlights a different aspect of the case.

Asymmetric Interdependence as a Source of Power?

The Japan-EU agreement on data transfer could be seen as one of mutual recognition as it involves reciprocal adequacy findings. However, policy adjustment for the "mutual" adequacy findings seems to be rather one-sided. While the APPI was not amended solely to meet the EU standards, the mutual recognition agreement would not have been possible without the amendment of the APPI.

Considering that the EU is the third-largest export market for Japan, its responsiveness to the EU's regulatory policy is not surprising. The Japanese government and its businesses were concerned with the data protection rules of the EU because of the opportunities its huge and thus potentially lucrative market might provide. In fact, the EU is one of the largest economies in the world, with a nominal gross domestic product (GDP) of roughly $19 trillion (IMF 2019). Furthermore, Japan depends on the EU market more than the EU depends on that of Japan. In 2016, while 12% of Japan's total exports were destined for the EU, exports to Japan accounted for only 3% of the total exports from the EU (European Commission 2018c). Thus, a structuralist argument of foreign pressure could be made in the context of the Japan-EU economic relationship, to the extent that the Japanese responsiveness to the EU's regulation could be attributed to Japan's dependence on the EU for the export market.[13]

However, Japan does have a relatively large domestic market, with a nominal GDP of around $5 trillion and a population of 127 million (IMF 2019;

13. This is consistent with the argument that a large domestic market allows the government overseeing it to exert regulatory influence on other countries. See Drezner (2007).

Statistics Bureau of Japan n.d.). This was presumably the main reason the EU decided to negotiate an EPA with Japan and, concomitantly, prioritized the data dialogue with Japan as a key trading partner in Asia. Furthermore, the EU seemingly made a concession for Japan by accepting "Japan's insular approach" (Greenleaf 2018, 11), which only applies stronger GDPR-like provisions to personal data that originate in the EU but does not extend to those originating in Japan. Significantly, Japan still lacks comprehensive data privacy legislation that covers both the public and the private sectors.

The International Interests of Domestic Firms

It is almost cliché to say that foreign policy behaviors and domestic politics are interrelated. According to the seminal work on the two-level game model, which is undoubtedly the most influential approach to analyzing interactions between domestic politics and international negotiations, "the potential reverberation of international pressures within the domestic arena" is one of the "significant features of the links between diplomacy and domestic politics" (Putnam 1988, 460). The importance of "reverberation" within domestic politics is underscored in the study of *gaiatsu*, which argues that foreign pressure is likely to be effective in bringing about a change in Japan, when the change is compatible with the preferences of influential domestic actors (Schoppa 1997). What, then, was the preference of the major domestic actors that would be affected by the Japan-EU data agreement, namely, personal information handling business operators in Japan?

Contrary to the conventional wisdom that the regulated industry prefers deregulation or, when regulation is lax enough, regulatory status quo, the Japanese business community was willing to accommodate changes in data protection regulation for the sake of "international harmonization." Behind this seemingly unusual policy stance was the transnationalization of Japanese firms. As Japanese firms expanded their businesses abroad, they became more dependent on transborder data flows. According to a study commissioned by the Ministry of Internal Affairs and Communications, approximately 40% of the Japanese firms surveyed said that they had made data transactions across borders (Ministry of Internal Affairs and Communications 2017).

As noted, data sent and received across borders include personal data. Indeed, transnational businesses——not only those in the IT sector but also in other sectors——transfer and use personal data (e.g., data containing

personal information of customers or employees) across borders to carry out activities such as marketing, the development of new products and services, and intra-firm management.

Since Japan was outside of the privileged group of countries with adequacy decisions, however, European subsidiaries of Japanese firms experienced some difficulties sending personal data to Japan. The problem was real. While some subsidiaries of Japanese firms in the EU went to the trouble of implementing additional safeguards, such as standard contractual clauses, others gave up the sharing of EU-originating data with entities located in Japan and set up a dedicated data processing center within the jurisdiction of the EU (Anonymous 2015).

Japanese businesses became even more concerned with the transfer of data from the EU after the GDPR was adopted in April 2016. To minimize the legal risks associated with the GDPR, Japanese businesses that had transactions with entities in the EU needed a framework that would allow them to smoothly transfer personal data from the jurisdiction of the EU to Japan. The stakes seemed extremely high. If their subsidiaries in the EU fail to comply with the GDPR, they will be sanctioned by the regulatory authorities of the EU (i.e., DPAs), and may face an administrative fine of up to € 20 million (US$ 22 million) or 4% of the total worldwide annual turnover of the preceding financial year.

Against this backdrop, Keidanren vocally demanded policy measures to facilitate the "mutual and smooth transfer of data" between Japan and the EU. Representing the business community in Japan, Keidanren on March 17, 2015, released a policy paper titled "Recommendations for Japan-EU Regulatory Cooperation: Looking Beyond Concluding the EPA/FTA." In this paper, Keidanren (2015, 13) argued that "[s]moother trans-border data flow would require, among other things, international harmonization of national and regional regulations and institutions related to appropriate treatment of personal data" and called for "consultation on rules for trans-border data transfer" with the EU. Understandably, such a demand from the business community served as a "tailwind" for the Japan-EU data transfer dialogue.[14]

14. Interview with an official of the PPC, March 13, 2019. It should be noted that "Japan does not have any IT giants," and consequently the Japanese government sought to create a legal environment that would support the transnational operations of "Japanese businesses at large, not specific firms." Interview with an official of the Ministry of Internal Affairs and Communications, April 5, 2017.

It was observed in the early 1990s that "with the increasing interdependence of economies, major interest groups often have international interests" (Krauss 1993, 292). The analysis above suggests that the international interests of influential domestic actors, that is, domestic businesses, are critical in the interaction between foreign pressure and domestic politics in the age of globalization.

The Transnational Politics of Regulation

Japanese firms were concerned with the EU's data protection rules because they had already taken advantage of the EU market or aspired to do so. In this regard, it is important to note that transnationalized Japanese firms were directly affected by the data protection regulation of the EU.

Needless to say, the subsidiaries of Japanese firms located in the EU must abide by its laws, because they are situated *within* the territorial jurisdiction of the EU. However, firms located in Japan and, thus, located *outside* of the EU are also affected by the data protection rules originating from Brussels, particularly the third-country transfer rule under the GDPR (previously the Data Protection Directive), if they are to receive personal data from the EU.

Technically speaking, the scope of application of the EU data protection laws is limited to the jurisdiction of the EU. Nonetheless, since EU data protection laws impose over-the-border obligations on transnational conduct (i.e., the trans-border transfer of personal data)—such that the personal data of EU citizens are protected wherever their data are transferred—they have "extra-jurisdictional" (Shaffer 2000, 55) or extraterritorial effects. In other words, EU data protection laws exercise a certain degree of control on the data processing operations of entities in foreign jurisdictions.

The extraterritorial effect arising from the application of the EU's data protection laws to data transfers beyond the border of the EU is key to understanding the reasons the Japanese business community urged the Japanese government to "consult" with the EU for an arrangement of mutual recognition, although it involved the upward convergence of regulation. For transnationalized Japanese businesses, the perceived benefit they might receive from the smooth transfer of personal data from the EU to Japan outweighed the expected adjustment cost entailed in complying with more-stringent data protection rules.

It should be noted that, in the case of data transfer between Japan and the EU, the EU's regulatory agencies, rather than its political actors, played a vital

part in creating the extraterritorial effect of the EU data protection regulation. While EU data protection laws' "extraterritorial provision prompted other countries . . . to reconsider their data privacy policies" (Newman 2008, 5), it was the formidable ability of European DPAs that gave the EU data protection regulation real teeth.[15] These "protectors of privacy" not only have the expertise to make recommendations on adequacy, but also the authority to impose sanctions. Specifically, DPAs have the statutory authority to block data flows to countries without "an adequate level" of privacy regulation, and thus can, in effect, deny access to the EU market for firms in these countries. This created an incentive for Japan to pursue the reform of personal information protection regulation to be found "adequate."

In sum, the extraterritorial effect of the EU's data protection regulation results from the imposition of over-the-border obligations, which is effectively ensured by European DPAs. The EU's regulation is relevant to Japanese firms precisely because they engage in activities that extend across the jurisdictions of both Japan and the EU. Therefore, it can be argued that the transnationalization of Japanese firms allowed the EU to exert regulatory influence on Japan and, conversely, increased Japan's responsiveness to the EU's regulatory pressure.

CONCLUSION

The policy process leading to the Japan-EU data transfer agreement illustrates how the external impetus for regulatory change can reverberate within domestic political systems. The analysis of the case in this study suggests that the latest changes in the Japanese personal information protection regulation were prompted by the influence of the EU's data protection regulation *and* the transnationalization of Japanese firms.

The EU's regulatory pressure concerning data protection penetrated the Japanese policy process by raising the stakes for transnationalized Japanese firms. As Japanese firms transnationalized their activities and made their way into the European market, they became susceptible to the extraterritorial effects of the EU's data protection rules, particularly third-country transfer rules. To mitigate the beyond-the-border effects of EU regulation, while pressing for more extensive use of personal information, the Japanese

15. For regulatory capacity, see Bach and Newman (2007) and Newman (2008).

business community called on the Japanese government to take measures to facilitate the smooth transfer of personal data from the EU to Japan. Business also acquiesced to the ratcheting-up of personal information protection standards as a condition for such data transfer.

The case of the Japan-EU data transfer dialogue confirms an argument inspired by the two-level game approach, which holds that "reverberation might increase international cooperation" (Putnam 1988, 455).[16] The findings of the analysis suggest that the reverberation of the EU's regulatory pressure within the domestic policy process of Japan precipitated the conclusion of a landmark agreement. In other words, the reverberation enhanced the regulatory cooperation between Japan and the EU.

One implication of this case analysis is that the study of foreign pressure could be broadened to take into consideration the extraterritorial effects of domestic or national regulation. As activities in the market undergo a transformation, the regulation of market-relevant activities, including data processing and transfers, is also changing, not only in terms of how they are made and implemented but also in terms of how they are altered in the face of external pressures. Conceivably, an investigation of extraterritorial regulatory pressure could contribute to the study of foreign pressure by adding to the knowledge related to the external impetus for change.

Theoretical arguments aside, it is worth noting that the locus of international data politics seems to be shifting from the Atlantic to the other side of the globe. Alerted by the rise of China as a data power, the Japanese government is now taking the initiative to establish common data privacy rules with the US and the EU in an attempt to create a zone of free data flows (Nikkei staff writers 2018). The basic idea is that data would flow freely among countries that have agreed to adhere to the common rules (e.g., Japan, the US, the EU countries, and perhaps more), but not to those deemed to fail to provide an adequate level of data protection. Thus, the system would be based on the adequacy principle of data transfer. However, the question is: will the US come to terms with the European data protection standards? With enormous economic interests involved, it is literally a million-dollar question.

16. The EU's tacit demand for a higher level of data privacy protection had "legitimacy," because Japan shared the view that privacy should be understood as a right of the people, "who shall be respected as individuals" (Japanese Constitution, Article 13). For an argument asserting that the perceived legitimacy of foreign pressure leads to positive reverberations within the domestic political process, see Schoppa (1997).

If Japan is to lead the trilateral efforts for free data flows, it must find a solution that is acceptable to both the US and the EU. In a sense, Japan is in a good position to accomplish this. To repeat one last time, Japan made a mutual adequacy arrangement with the EU that is expected to "serve as an example for future partnerships in this key area" (European Commission 2019b). At the same time, as a member economy of the Asia-Pacific Economic Cooperation (APEC) forum, Japan has endorsed the APEC Privacy Framework, which bears a strong imprint of US "leaning toward less exacting data protection" (Bennett and Raab 2006, 105). Under the APEC Privacy Framework, personal information may be transferred internationally or domestically so long as a personal information controller is *accountable* for ensuring that the recipient will protect the information. Thus, Japan is positioned at the intersection of the European principle of adequacy and the Asia-Pacific (or rather the US) principle of accountability. For now, however, the role Japan will play in the emerging international data transfer regime remains to be seen.

REFERENCES

Anonymous. 2015a. "Kojin joho hogo obei to zure, EU no kinshi sochi tekkai he kosho hoshin" [Discrepancies with American and European personal information protection, negotiation policy to have the EU's prohibitive measures lifted]. *Asahi Shimbun*, May 16, 2015.

Anonymous. 2015b. "Nihon kigyo oshu kyoten no kojin joho nihon de kanri kano ni" [Japanese firms to be allowed to domestically process personal information held by their European subsidiaries]. *Nihon Keizai Shimbun*, September 15, 2015.

Anonymous. 2017a. "Nichio deta iten rai-shun goi mezasu" [Japan-Europe data transfer set to be agreed upon next spring]. *Nihon Keizai Shimbun*, December 14, 2017.

Anonymous. 2017b. "Kojin joho no iten nichio de shishin sakusei" [Japan and Europe to develop a guideline for the transfer of personal information]. *Nihon Keizai Shimbun*, December 15, 2017.

Anonymous. 2018. "Hokanteki ruru de EU-nami ni hogo" [EU-equivalent protection with supplementary rules]. *Nihon Keizai Shimbun*, October 22, 2018.

Article 29 Data Protection Working Party. 2001. *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*. WP40 final.

Bach, David and Abraham L. Newman, 2007. "The European regulatory state and global public policy: micro-institutions, macro-influence." *Journal of European Public Policy* 14 (6): 665–695.

Bennett, Colin J. 1998. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" In *Technology and Privacy: The New Landscape*, eds. Philip E. Agre and Marc Rotenberg. Cambridge, MA: MIT Press.

Bennett, Colin J. and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge. MA: MIT Press.

Calder, Kent. 1988. "Japanese Foreign Economic Policy Formation: Explaining the Reactive State." *World Politics* 40 (4): 517–541.

Council of the European Union. 2009. *The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens*.

European Commission. 2012. *Proposal for a Regulation of the European Parliament and the of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. COM(2012) 11 final.

European Commission. 2017. *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*. COM(2017) 7 final.

European Commission. 2018a. "The European Union and Japan agreed to create the world's largest area of safe data flows." Accessed February 4, 2019. https://europa.eu/rapid/press-release_IP-18-4501_en.htm.

European Commission. 2018b. "International data flows: Commission launches the adoption of its adequacy decision on Japan." Accessed October 27, 2018. http://europa.eu/rapid/press-release_IP-18-5433_en.htm.

European Commission 2018c. *The Economic Impact of the EU-Japan Economic Partnership Agreement (EPA): An analysis prepared by the European Commission's Directorate-General for Trade.* Accessed July 14, 2019. https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157116.pdf.

European Commission. 2019a. *Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information*. C(2019) 304 final.

European Commission. 2019b. "European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows." Accessed February 4, 2019. http://europa.eu/rapid/press-release_IP-19-421_en.htm.

European Data Protection Board (EDPB). 2018. *Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan*.

European Parliament. 2014. *European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. P7_TA(2014)0212.

Drezner, Daniel W. 2007. *All Politics Is Global: Explaining International Regulatory Regimes.* Princeton: Princeton University Press.

Farrell, Henry. 2003. "Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement." *International Organization* 57 (2): 277–306.

Farrell, Henry and Abraham L. Newman. 2019. *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*. Princeton, Princeton University Press.

Greenleaf, Graham. 2018. "Japan and Korea: Different paths to EU adequacy." *Privacy Laws & Business International Report* 156: 9–11.

International Monetary Fund (IMF). 2019. *World Economic Outlook*. Accessed July 14, 2019. https://www.imf.org/external/pubs/ft/weo/2019/01/weodata/index.aspx.

Information Technology (IT) Strategic Headquarters. 2004. *Policy Outline of the Institutional Revision for Utilization of Personal Data*. Accessed February 20, 2019. https://japan.kantei.go.jp/policy/it/20140715_2.pdf.

Kawabata, Eiji. 2016. "Privacy Governance in Japan." In *Information Governance in Japan: Towards a New Comparative Paradigm*, edited by Kenji E. Kushida, Yuko Kasuya, and Eiji Kawabata, 249–283. Stanford: Stanford Silicon Valley New Japan Project E-book Series. https://ssrn.com/abstract=3046663.

Keidanren. 2015. *Recommendations for Japan-EU Regulatory Cooperation: Looking Beyond Concluding the EPA/FTA*. Accessed June 1, 2015. https://www.keidanren.or.jp/policy/2015/024_honbun.html.

Keidanren. 2018. "Chairman Nakanishi's Comments on the Signature of the Japan-EU Economic Partnership Agreement (EPA)." Accessed February 10, 2019. http://www.keidanren.or.jp/en/speech/comment/2018/0717.html.

Kobrin, Stephen J. 2004. "Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance." *Review of International Studies* 30 (1): 111–131.

Krauss, Ellis S. 1993. "U.S.-Japan Negotiations on Construction and Semiconductors, 1985–1988: Building Friction and Relation-Chips." In *Double-Edged Diplomacy: International Bargaining and Domestic Politics,* edited by Peter B. Evans, Harold K. Jacobson, and Robert D. Putnam, 265–299. Berkeley: University of California Press.

McKinsey Global Institute. 2016. *Digital Globalization: The New Era of Global Flows*. Accessed February 11, 2019. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

Ministry of Foreign Affairs of Japan. 2013. "Japan-EU Summit Telephone Talks." Accessed October 27, 2018. https://www.mofa.go.jp/region/page5e_000023.html.

Ministry of Internal Affairs and Communications. 2017. *White Paper 2017 Information and Communications in Japan*. Accessed February 6, 2019. http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2017/chapter-2.pdf#page=9.

Ministry of Justice, Cabinet Secretariat, National Police Agency, Personal Information Protection Commission, Ministry of Internal Affairs and Communications, Public Security Intelligence Agency, and Ministry of Defense. 2018. "Collection and use of personal information by Japanese public authorities for criminal law enforcement and national security purpose." Accessed June 1, 2019. https://www.ppc.go.jp/files/pdf/letter_government_access.pdf.

Newman, Abraham L. 2008. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca: Cornell University Press.

Nikkei staff writers. 2018. "Japan, US and EU to establish data transfer rules: Nations seek privacy safeguards and to block personal data flows to China." *Nikkei Asian Review*. December 18, 2018. Accessed February 6, 2019. https://asia.nikkei.com/Economy/Japan-US-and-EU-to-establish-data-transfer-rules.

Personal Information Protection Commission (PPC). 2017. "Press statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission." Accessed March 15, 2019. https://www.ppc.go.jp/files/pdf/290704_press statement.pdf.

PPC. 2018a. "Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission." Accessed March 15, 2019. https://www.ppc.go.jp/files/pdf/300531_pressstatement.pdf.

PPC. 2018b. "Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission." Accessed March 15, 2019. https://www.ppc.go.jp/files/pdf/300717_pressstatement2.pdf.

PPC. 2019. "The framework for mutual and smooth transfer of personal data between Japan and the European Union has come into force." Accessed February 4, 2019. https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/.

PPC. n.d.a. "Chairman Masao Horibe." Accessed July 15, 2019. https://www.ppc.go.jp/en/aboutus/commission/chairman/.

PPC. n.d.b. "Iken boshu" [Calls for public comments]. Accessed February 24, 2019. https://www.ppc.go.jp/news/public-comment/.

PPC. n.d.c. "Dai-85-kai kojin joho hogo iinnkai" [85th meeting of the Personal Information Protection Committee]. Accessed July 4, 2019. https://www.ppc.go.jp/aboutus/minutes/2018/20190118/.

Putnam, Robert D. 1988. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42 (3): 427–460.

Reidenberg, Joel R. 2000. "Resolving Conflicting International Data Privacy Rules in Cyberspace." *Stanford Law Review* 52 (5): 1315–71.

Schoppa, Leonard J. 1997. *Bargaining with Japan: What American Pressure Can and Cannot Do*. New York: Columbia University Press.

Shaffer, Gregory. 2000. "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards." *Yale Journal of International Law* 25 (1): 1–88.

Statistics Bureau of Japan. n.d. *Population and Households of Japan 2015*. Accessed July 14, 2019. https://www.stat.go.jp/english/data/kokusei/2015/poj/mokuji.html.

White House. 2012. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Accessed February 20, 2019. https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.