Harvard Journal of Law & Technology
Volume 33, Number 2 Spring 2020

COOPERATIVE DATA PRIVACY: THE JAPANESE MODEL OF DATA PRIVACY AND THE EU-JAPAN GDPR ADEQUACY AGREEMENT

*Flora Y. Wang**

TABLE OF CONTENTS

I. INTRODUCTION

In a January 2019 speech at the World Economic Forum in Davos, Prime Minister Shinzo Abe announced that "the engine for growth" was "fueled no longer by gasoline, but more and more by digital data."[1]

---

* Harvard Law School, J.D. Candidate Class of 2020; Stanford B.A. in International Relations with Honors in International Security, 2013; Fulbright Scholar. I am deeply grateful to Professor Chris Bavitz for advising the paper which led to this Note and for his kind guidance and mentorship. My sincere thanks to Article Editor Or-el Vaknin for his excellent insights and comments and to the editorial staff of the Harvard Journal of Law & Technology for their contributions to this Note. I would also like to thank my interviewees for their generosity and patience, and in particular Professor Kaori Ishii, Professor Fumio Shimpo, and Shintaro Kobayashi for their invaluable expertise. My thanks to Professor Mark Wu, Professor Jacques deLisle, and Professor Alvaro Santos for their comments on my presentation of a draft of this paper at the Salzburg Cutler Fellowship Conference in February 2020, and to Professor Urs Gasser, Professor Sandra Wachter, Andrei Gribakov Jaffe, and Vinny Mei for their kind advice. This research was generously supported by the Cravath International Fellowship. This Note is dedicated to my family for their love and support. All opinions and errors are my own.

1. Shinzo Abe, Prime Minister of Japan, Toward a New Era of "Hope-Driven Economy": the Prime Minister's Keynote Speeach [sic] at the World Economic Forum Annual Meeting (Jan. 23, 2019), http://japan.kantei.go.jp/98_abe/statement/201901/_00003.html

He called for the international community to establish a global infrastructure that would "enable the free flow of medical, industrial, traffic and other most useful, nonpersonal, anonymous data to see no borders."[2] At the G20 Summit in June 2019, he introduced the launch of an "Osaka Track" framework for data governance by emphasizing that "rule-making on data flow and e-commerce, which are the growth engines in the digital area, is an urgent mission."[3]

Abe's speech highlights the importance of data governance in the era of machine learning and artificial intelligence. Data privacy is crucial for technological innovation, economic prosperity, national security, and human rights.[4] Without a "common international rule" for data privacy,[5] "the rules for who controls data — and therefore harnesses their value — are part of a bigger geopolitical competition."[6] The current discourse on global data privacy reform has tended to focus on the European Union ("EU"), the U.S., and the Chinese models of data privacy. The "privatized" approach favored by the United States sharply contrasts with China's state-controlled framework, with its expansive surveillance powers.[7] German Chancellor Angela Merkel argues that the EU occupies a middle ground between these two opposing models.[8] However, under Prime Minister Abe, Japan has been intentionally positioning itself as a leader in the worldwide race to determine data protection rules.[9] Japan's model of cooperative data privacy serves as an

---

[https://perma.cc/HZ9D-PD9K]; *see also* Daniel Hurst, *Japan Calls for Global Consensus on Data Governance*, DIPLOMAT (Feb. 2, 2019), https://thediplomat.com/2019/02/japan-calls-for-global-consensus-on-data-governance [https://perma.cc/6CC5-PTRT].

2. Shinzo Abe, *"Defeatism About Japan is Now Defeated": Read Abe's Davos Speech in Full*, WORLD ECON. F. (Jan. 23, 2019), https://www.weforum.org/agenda/2019/01/abe-speech-transcript [https://perma.cc/A8TH-YXUY]; *see also* Hurst, *supra* note 1.

3. Satoshi Sugiyama, *Abe Heralds Launch of "Osaka Track" Framework for Free Cross-Border Data Flow at G20*, JAPAN TIMES (June 28, 2019), https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20 [https://perma.cc/PG66-MRFW].

4. *See* Samm Sacks & Justin Sherman, *The Global Data War Heats Up*, ATLANTIC (June 26, 2019), https://www.theatlantic.com/international/archive/2019/06/g20-data/592606 [https://perma.cc/5T63-5N25].

5. Heizo Takenaka, *The Global Battle Over Big Data*, JAPAN TIMES (Mar. 5, 2019), https://www.japantimes.co.jp/opinion/2019/03/05/commentary/japan-commentary/global-battle-big-data [https://perma.cc/84K9-M2GF].

6. *See* Sacks & Sherman, *supra* note 4.

7. *See Can the EU Become Another AI Superpower?*, ECONOMIST (Sept. 20, 2018), https://www.economist.com/business/2018/09/20/can-the-eu-become-another-ai-superpower [https://perma.cc/Q79J-M78R].

8. *Id.*

9. *See* Sacks & Sherman, *supra* note 4; Masumi Koizumi, *Japan's Pitch for Free Data Flows "With Trust" Faces Uphill Battle at G20 Amid "Splinternet" Fears*, JAPAN TIMES (June 27, 2019), https://www.japantimes.co.jp/news/2019/06/27/business/tech/japans-pitch-free-data-flows-trust-faces-uphill-battle-g20-amid-splinternet-fears [https://perma.cc/97MS-CHEX].

important, alternative precedent in the rapidly evolving field of international data privacy and geopolitical competition over data governance.

The most significant way in which Japan has been advocating for a new model of data protection and the free flow of data has been through the adoption of the landmark General Data Protection Regulation Adequacy Decision between the European Union and Japan ("the Adequacy Decision").[10] The Adequacy Decision is groundbreaking, as it is not only the first adequacy agreement signed after the implementation of the General Data Protection Regulation ("GDPR"),[11] but also the first mutual adequacy agreement between the EU and a non-EU country.[12] The EU recognized the Japanese Act on the Protection of Personal Information ("APPI")[13] as providing an "equivalent" level of protection as the GDPR.[14] Once the European Commission ("Commission") adopts an adequacy decision and it comes into effect, "personal data can flow safely from the European Economic Area ("EEA") (the 28 EU Member States as well Norway, Liechtenstein, and Iceland) to that third country, without being subject to any further safeguards or authorizations."[15] This recognition of mutual adequacy is significant. Until this point, Europe had "covered only the flow of personal data from the EU to [a] non-EU entity," but not flows from the non-EU entity back to the EU.[16] Extensive data flow of this scale in both directions between two parties is unique. The Adequacy Decision serves as "a precedent for future adequacy applications as well as for the review of adequacy decisions rendered under Directive 95/46."[17]

---

10. *See* Commission Implementing Decision (EU) 2019/419 of 23 January 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, 2019 O.J. (L 76) 1 [hereinafter Commission Implementing Decision].

11. Regulation 2016/679 of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

12. *Questions & Answers on the Japan Adequacy Decision*, EUROPEAN COMM'N 1 (Jan. 23, 2019), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_19_422/MEMO_19_422_EN.pdf [https://perma.cc/G8XA-M5XZ] [hereinafter *Questions & Answers*].

13. Kojin jōhō no hogo nikansuru hōritsu [Amended Act on the Protection of Personal Information], Law No. 57 of 2003, translated in PERS. INFO. PROTECTION COMM'N, AMENDED ACT ON THE PROTECTION OF PERSONAL INFORMATION (TENTATIVE TRANSLATION), VER. 2, at 5 (2016) [hereinafter Amended APPI].

14. *Questions & Answers*, *supra* note 12, at 1.

15. *Id.*

16. Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 790 (2019).

17. European Data Prot. Bd., Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan, ¶ 28 (Dec. 5, 2018), https://edpb.europa.eu/sites/edpb/files/files/file1/2018-12-05-opinion_2018-

This Note presents the Japanese model of cooperative data privacy as a precedent for countries seeking to reform their legal regimes in the wake of the GDPR. It examines this model through the remarkable story of the Adequacy Decision and data privacy from the Japanese perspective. There is extensive literature on the GDPR and its implications for global privacy regulation.[18] In addition, there is some Western scholarship on the Japanese concept of privacy.[19] However, this Note aims to fill the gap between the two by connecting the GDPR Adequacy Decision — and the process leading up to it — with the Japanese view on data privacy and enforcement. It also argues that Japan's cooperative but restrictive approach in response to the "Brussels Effect" can serve as a model for other countries. The Note draws from interviews with Japanese data privacy experts in Tokyo, which occurred prior to the adoption of the Adequacy Decision, but shortly after negotiations wrapped up in Japan.[20]

This Note tells the story of the Japanese cooperative data privacy model and the Adequacy Decision in five main parts. Part II introduces the GDPR framework and the debate over its impact on global privacy norms. Part III discusses the collision and convergence of the EU and Japanese data privacy regimes. Part IV explores the growing tension between foreign companies and local culture, and the role that reputational risks play in Japanese enforcement mechanisms. Part V argues that Japan can serve as a key model for countries weighing the merits of competing regulatory frameworks in the absence of universal data

---

28_art.70_japan_adequacy_en.pdf [https://perma.cc/ZWS3-CTMH] [hereinafter Opinion of the Board] (emphasis omitted).

18. *See, e.g.*, Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 22–26 (2012); William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 967–70 (2016); Cedric Ryngaert, *Symposium Issue on Extraterritoriality and EU Data Protection*, 5 INT'L DATA PRIVACY L. 221, 223 (2015) ("Underneath the jurisdictional discourse, dominated by such concepts as territoriality, effects, and personality, lies a more substantive discourse regarding the appropriate balance to be struck between data protection and other societal goals, such as security (for example, fighting terrorism or cybercrime) and facilitating transnational business."); Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019); Graham Greenleaf, *International Data Privacy Agreements After the GDPR and* Schrems (Univ. of N.S.W. Law Research Series, Paper No. 29, 2016).

19. *See, e.g.*, Charles Ess, *"Lost in Translation"?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia)*, 7 ETHICS & INFO. TECH. 1, 3–4 (2005); Graham Greenleaf & Fumio Shimpo, *The Puzzle of Japanese Data Privacy Enforcement*, 4 INT'L DATA PRIVACY L. 139 (2014); Hiroshi Miyashita, *The Evolving Concept of Data Privacy in Japanese Law*, 1 INT'L DATA PRIVACY L. 229 (2011); Makoto Nakada & Takanori Tamura, *Japanese Conceptions of Privacy: An Intercultural Perspective*, 7 ETHICS & INFO. TECH. 27 (2005); Schwartz, *supra* note 16, at 786–92; Motohiro Tsuchiya, *Systematic Government Access to Private-Sector Data in Japan*, 2 INT'L DATA PRIVACY L. 239 (2012); Graham Greenleaf, *2017-2018 Further Update to Graham Greenleaf's Asian Data Privacy Laws — Trade and Human Rights Perspectives* 8–10 (Univ. of N.S.W. Law Research Series, Paper No. 4, 2019).

20. The interviews were found to be exempt by the Harvard Institutional Review Board ("IRB").

privacy standards. This Note predicts that Japan will revise the Adequacy Decision in 2021 (with periodic review at least every four years), which will likely increase the Japanese data protection authority's enforcement powers. However, such legal reforms will probably be limited and primarily be in reaction to external pressure from the international community. Domestic resistance within Japan to a wholesale importation of the EU data privacy system creates a reactive, two-track model that both provides economic benefits and cabins the extent of domestic reforms. The Adequacy Decision highlights the complexities of data governance across two disparate cultures, value systems, and concepts of privacy. However, the Adequacy Decision is also significant for illustrating the limited success of the European Union's vision of utilizing the GDPR to establish global human rights standards. This unique Japanese model suggests that states can pursue a cooperative approach to data privacy that maintains domestic values, culture, and identity — all while also benefiting economically from data flows.

II. THE SIGNIFICANCE OF THE EU'S GDPR DATA PRIVACY FRAMEWORK

The GDPR has important precedent-setting effects for future European negotiations and extraterritoriality. In April 2016, the EU replaced the 1995 Data Protection Directive with the GDPR, which came into effect on May 25, 2018.[21] The GDPR drastically changed the regulatory landscape of data privacy, primarily due to its territorial scope.[22] The GDPR's restrictions apply to all businesses which "process[] personal data in the context of the activities of an establishment of a controller or a processor in the Union," even if such processing occurs outside the EU.[23] In addition, the GDPR "recognized for the first time in European legislative history" the following obligations: "collective redress, wealth-based punishment, and arming data subjects with the right to initiate public enforcement."[24] The EU intentionally uses its market power as the world's largest trading bloc with 500 million consumers to integrate with other data privacy regimes and establish a more EU-favorable structure for such agreements.[25] Former European Parliament Member Julia Reda stated that the GDPR purposefully "uses the market to set human rights standards. If the other

21. *See* GDPR, *supra* note 11, at art. 99.

22. *See id.* at art. 3 (setting territorial scope of regulation's effect).

23. *Id.*

24. Rustad & Koenig, *supra* note 18, at 368–69.

25. *See EU Position in World Trade*, EUROPEAN COMMISSION, (Feb. 18, 2019) https://ec.europa.eu/trade/policy/eu-position-in-world-trade [https://perma.cc/U9RU-VYTK].

parts of the world decide to pursue data protection out of business interest, that is exactly what [the European Parliament] want[ed] to achieve."[26] As other countries' privacy rules are measured against the GDPR, this de facto global standard has sparked ripple effects around the world.[27]

The extent of the GDPR's influence on non-EU domestic privacy regimes is the subject of significant debate. Professor Graham Greenleaf believes the "3rd Generation of evolving global data privacy standards" will be decided by "which of [the GDPR's] new content principles and enforcement requirements are likely to become standard elements of data privacy laws outside the EU."[28] Professor Anu Bradford defines "Europe's unilateral power to regulate global markets" as the "Brussels Effect" phenomenon.[29] According to Professor Bradford, Europe "externalize[s] its laws and regulations outside its borders through market mechanisms, resulting in the globalization of standards."[30] She characterizes this process of one state's actions in the global market as "unilateral regulatory globalization."[31] She argues that "[w]hile the EU regulates only its internal market, multinational corporations often have an incentive to standardize their production globally and adhere to a single rule."[32] This dynamic converts the EU rule into a global standard, which Bradford calls the "de facto Brussels Effect."[33] She claims that this in turn produces the "de jure Brussels Effect," as "after these export-oriented firms have adjusted their business practices to meet the EU's strict standards, they often have the incentive to lobby their domestic governments to adopt these same standards in an effort to level the playing field against their domestic . . . competitors."[34] Therefore, Europe can export its privacy standards to another jurisdiction, even without the latter actively imposing it.[35] Professors Michael Rustad and Thomas Koenig explore the GDPR as a case study of the impact of the Brussels Effect on the field of data privacy. They suggest that the GDPR could "become the basis of a worldwide 'gold standard'

26. Julia Reda, Fellow, Berkman Klein Ctr., Speech and Q&A Session at Harvard Law School (Sept. 20, 2019).

27. Ryan Johnson & Logan Finucan, *The Europeans Are Winning the Global Privacy Debate*, TREASURY & RISK (Oct. 11, 2018, 8:59 AM), https://www.treasuryandrisk.com/2018/10/11/the-europeans-are-winning-the-global-privacy-debat [https://perma.cc/BX8R-TMH5].

28. Greenleaf*, supra* note 18, at 5.

29. Bradford, *supra* note 18, at 3.

30. *Id.*

31. *Id.*

32. *Id.* at 6.

33. *Id.*

34. *Id.*

35. *Id.* at 4.

for global data privacy."[36] Moreover, they claim that the Brussels Effect can lead to a "'race to the top' as multinational entities find it easier to apply the strongest data protection standards worldwide, rather than satisfying divergent data privacy rules."[37]

Contrary to Professor Bradford's vision of the EU exerting unilateral power through its market share, Professor Paul Schwartz argues that the experiences of Japan and the United States in seeking GDPR adequacy agreements counters the Brussels Effect hypothesis.[38] Instead, Schwartz suggests that there is a "varied range of nation-state, transnational, and corporate behavior that has helped spread EU data protection throughout the world."[39] He claims that "[t]he case studies show openness to varied and customized approaches, rather than rigid exercises of unilateral de facto power."[40] While "the EU's adequacy requirement has provided the EU with important negotiating leverage," the Japan and the U.S. case studies "demonstrate that the EU's regulatory capacity arises from a complex interplay among EU institutions and outside influences," rather than the EU "exercising power as a monolithic entity."[41] Schwartz suggests that "the process of reaching an adequacy agreement proved to be neither unilateral nor de facto," as "Japan chose to engage in bilateral negotiations with the EU and create a reciprocal agreement."[42] He further claims that "the result is de jure, not de facto law," as "[t]he commitments were carefully documented in the APPI and the Annexes to the Commission Implementing Decision."[43] He also argues that the Adequacy Decision disproves Bradford's Brussels Effect timeline, because Japan compared the GDPR against other data privacy models and decided to "affirmatively [choose] a system similar and compatible with EU data protection law."[44]

III. THE COLLISION & CONVERGENCE OF PRIVACY REGIMES

Given the EU and Japan's disparate concepts of data privacy, as well as distinct political and legal systems, the Adequacy Decision is a remarkable achievement. The following sections present the story of

36. Rustad & Koenig, *supra* note 18, at 366. Though Professors Rustad and Koenig acknowledge the Brussels Effect on U.S. privacy law, they also claim that there is an "overlooked 'D.C. Effect' reflected in the GDPR's adoption of many U.S. data privacy innovations." *Id.* at 366–67, 371.

37. *Id.* at 370.

38. Schwartz, *supra* note 16, at 786, 803–805, 818.

39. Schwartz, *supra* note 16, at 773.

40. *Id.* at 774.

41. *Id.*

42. *Id.* at 803–04.

43. *Id.*

44. *Id.* at 804.

the Adequacy Decision and concurrent debates over data privacy from the perspective of Japanese data privacy experts. Section III.A discusses the different concepts of data privacy between Europe and Japan. Section III.B examines the Adequacy Decision as an example of the political, cultural, and legal difficulties of harmonizing two distinct privacy regimes. Section III.C explores the Personal Information Protection Commission ("PPC") Guidelines as a case study of cultural clashes that emerged during the adequacy negotiations and their resolution.

A. Japan and Europe: Disparate Concepts of Data Privacy

The most significant difference between the EU approach and the Japanese approach to privacy is that the EU considers data protection and privacy to be fundamental rights, viewing those rights as a more dominant rationale for regulation than economic incentives.[45] Though the EU acknowledges that privacy is an important part of international trade,[46] EU privacy regulations demonstrate that "European legal sources tend to view control over personal data as an inherent aspect of individual dignity."[47] The Charter of Fundamental Rights of the European Union ("the European Charter") is notable for protecting "[b]oth privacy and data protection."[48] In conjunction with the European Charter, other European constitutional documents and treaties also name privacy as a crucial right.[49] Consistent with this view, the EU declared in the press release regarding the EU-Japan Economic Partnership Decision that "[d]ata protection is a fundamental right in the European Union and is therefore not up for negotiation. Privacy is not a commodity to be traded."[50] Rustad and Koenig suggest that this cultural perspective primarily stems from a reaction to the Nazi "total surveillance state from 1933–1945," which permitted "unprecedented oppression" in Europe.[51]

---

45. *See* McGeveran, *supra* note 18, at 967 ("This concept can be attributed in part to continental political and cultural development of the idea that personal reputation and honor are central to human flourishing.").

46. *See Questions & Answers*, *supra* note 12, at 1.

47. *See* McGeveran, *supra* note 18, at 967.

48. Rustad & Koenig, *supra* note 18, at 373 ("Article 7 of the Charter recognizes general privacy protection for individuals by granting all Europeans 'the right to respect for his or her private and family life, home and communications.' Article 8 expressly recognizes the right to protection of personal data . . . .") (footnotes omitted).

49. McGeveran, *supra* note 18, at 967. The GDPR "expands and builds the individual rights," such as the right to be forgotten, the right to object, the right to rectification, the right of portability, the right of access, and the right to be notified. Rustad & Koenig, *supra* note 18, at 377.

50. Press Release, European Comm'n, Key Elements of the EU-Japan Economic Partnership Agreement (Apr. 18, 2018), https://europa.eu/rapid/press-release_MEMO-18-3326_en.htm [https://perma.cc/ECC7-6AFR] [hereinafter Key Elements].

51. Rustad & Koenig, *supra* note 18, at 372.

In contrast to Europe, the Japanese privacy framework emphasizes the importance of data as an economic commodity and protects a narrower range of personal information. Article 13 of the Japanese Constitution and subsequent tort case law implicitly recognize the right to privacy.[52] However, Article 13 of the Japanese Constitution strikes a very different tone from the European Charter, as unlike the latter, it omits any explicit references to the right of privacy or data protection.[53] Though the first sentence of Article 1 of the APPI (the most significant Japanese data privacy legislation) emphasizes that it "aims to protect the rights and interests of individuals,"[54] it also explicitly states that the economic salience of data serves a "secondary purpose."[55] The same sentence declares that the "proper and effective use of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life."[56] Moreover, the APPI protects only *personal information*, which provides a narrower scope of protection than a general right to privacy and data protection under the GDPR.[57] The scope of protected data for personal information is limited to "information relating to a living individual" (such as "name, date of birth, or other descriptions") which permits the "[identification of] a specific individual" or "those containing an individual identification code."[58] The GDPR defines personal data as "any information relating to an identified or identifiable natural person" that potentially identifies the individual.[59] Moreover, all computer cookie IDs and IP addresses are typically protected under European law's definition of personal data.[60] By contrast, the APPI does not protect computer cookie IDs and IP addresses as personal information if "they

52. Interview with Nobuyuki Sato, Professor, Chuo Law Sch., in Tokyo, Japan (Jan. 16, 2019).

53. *Id.*; *see also* Email from Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., to author (Dec. 30, 2019, 6:00 AM) (on file with author) ("In the past trial concerning the basic resident register network system, right to self-data control was once approved in the lower court, though, the supreme court has never approved it so far."); *compare* NIHONKOKU KENPŌ [KENPŌ] [CONSTITUTION], art. 13 (Japan) ("All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs."), *with* Charter of Fundamental Rights of the European Union arts. 7, 8, Dec. 7, 2000, 2010 O.J. (C 83) 389, 393.

54. Amended APPI, art. 1.

55. Email from Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., to author (Dec. 29, 2019, 5:00 PM) (on file with author).

56. Amended APPI, art. 1.

57. *Id.* The APPI's protections do not extend to the public sector. *Id.*

58. Amended APPI, art. 2.

59. GDPR, *supra* note 11, at art. 4.

60. GDPR, *supra* note 11, at ¶ 30 ("Natural persons may be associated with online identifiers . . . such as internet protocol addresses, cookie identifiers."); *see also* EUROPEAN COMMISSION, "What is Personal Data?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [https://perma.cc/RMY2-LM52]; Kobayashi Email, *supra* note 55.

cannot be readily collated with other information and thereby identify a specific individual."[61]

According to Professor Katsuya Uga, the APPI has a narrower definition of personal information "out of concern for the freedom of business in the private sector and in the interest of avoiding an overly broad regulation" of business operators handling personal information.[62] Professor Uga's perspective is significant, as he served as "a core member of the design of the first APPI in 2003 and also chairman of its revisions in 2015."[63] Thus, it is clear through the scope and tone of the Japanese Constitution and the APPI that Japan places more significant emphasis on the economic salience of data than the EU.

Prime Minister Abe's speech at Davos, which focused on the economic benefits of data privacy regulation, together with the APPI's tone, suggests that Japan primarily views privacy as a commodity for business opportunities.[64] As Professor Kiyoshi Murata sums up, "Japanese data protection law systems are not for privacy, but pro-economy."[65] Therefore, the Adequacy Decision represents the convergence of two distinct conceptions of data privacy — that of Japan and that of the EU. As discussed below, the controversy over using the PPC Guidelines as an enforcement mechanism further illustrates how the cultural, political, and legal differences between two parties affect data privacy negotiations.

B. The EU-Japan GDPR Adequacy Decision

The EU-Japan GDPR Adequacy Decision represents a new model of cooperative data privacy. The Adequacy Decision is the first time that an adequacy agreement has been adopted by the EU and another country (allowing EU data to flow to a non-EU entity) since the GDPR came into effect. It is also the first time that the EU has allowed data flows from a non-EU entity to the EU via a mutual adequacy decision.[66] A finding of adequacy is a decision taken by the European Commission that affirms "that a third country provides a comparable level of protection of personal data to that in the European Union."[67] For the first time, the EU acknowledged another country as providing an "essential[ly]

61. Email from Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., to author (Mar. 29, 2020, 7:45 PM) (on file with author).

62. KATSUYA UGA, PERSONAL INFORMATION PROTECTION ACT: ARTICLE BY ARTICLE 34 (6th ed. 2018) (Uga is now a Japanese Supreme Court Justice).

63. Email from Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., to author (Jan. 20, 2020, 5:26 PM) (on file with author).

64. *See* Abe, *supra* note 2.

65. Interview with Kiyoshi Murata, Professor and Dir. of the Ctr. for Bus. Info. Ethics, Meiji University, in Tokyo, Japan (Jan. 18, 2019) [hereinafter Murata Interview].

66. *See Questions & Answers*, *supra* note 12, at 2; Schwartz, *supra* note 16, at 790.

67. *Questions & Answers*, *supra* note 12, at 1.

equivalen[t]" level of data protection to the GDPR under a mutual adequacy agreement.[68] In a reciprocal manner, Japan acknowledged that the EU provides an adequate level of protection under the APPI.[69] Therefore, "[t]his finding of mutual reciprocity represents a new high point for the diffusion of the EU data protection model."[70] The Adequacy Decision "create[d] the world's largest area of safe and free data transfer based on a high level of protection."[71]

The Adequacy Decision is the product of a two-year process that began with negotiations in January 2017 and concluded with an agreement entering into effect in January 2019.[72] "The Commission published a draft adequacy decision in September, 2018; and the European Data Protection Board published its opinion of approval in December, 2018."[73] The European Data Protection Board ("EDPB") advises the European Commission "on any issue related to data protection in the EU," and provides it "with an opinion on the assessment of the adequacy of the level of protection in a third country."[74]

The Adequacy Decision appended additional regulations to a parallel Japanese data privacy act. The EU and Japan touted that the Adequacy Decision "build[s] on the high degree of convergence between the two systems," each of which relies on "an overarching privacy law, a core set of individual rights and enforcement by an independent data protection authority."[75] The EU and Japan primarily bridged the gap

68. *Id.*

69. *Questions & Answers*, *supra* note 12, at 1–2. *See also* Opinion of the Board, *supra* note 17, ¶ 42.

70. *Schwartz, supra* note 16, at 790.

71. *Questions & Answers*, *supra* note 12, at 1–2; *see also* European Commission Press Release IP/19/421, The Commission, European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (Jan. 23, 2019) [hereinafter European Commission Adopts].

72. *See* Schwartz, *supra* note 16, at 787. In 2015, Japan made significant legal amendments to the APPI, which "moved it significantly closer to the EU system." *Id.* at 788.

73. *Id.* at 787 (footnote omitted).

74. *Role of the EDPB*, EUROPEAN DATA PROT. BD., https://edpb.europa.eu/role-edpb_en [https://perma.cc/7RBY-T6BG].

75. *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*, PERS. INFO. PROT. COMMISSION (Jan. 23, 2019), https://www.ppc.go.jp/files/pdf/310123_pressstatement_en.pdf [https://perma.cc/GK6W-Z3K9].

between the two data privacy frameworks by appending the Supplementary Rules to the APPI in a separate annex.[76] The APPI is the fundamental legal cornerstone of the Japanese privacy framework.[77] The statute "provides the basic principles for the government's regulatory authority, as well as the obligations of private business owners who handle personal information."[78]

Japan made two concessions in the Supplementary Rules to satisfy the EU's adequacy requirements. First, Japan agreed to begin classifying sexual orientation and trade union membership status as sensitive data, contrary to prior practice.[79] Second, the Supplementary Rules "ensure that data subject rights will apply to all personal data transferred from the EU, irrespective of their retention period," even though Japanese law does not provide such protections.[80] This "insular" adequacy model contrasts with the South Korean approach, which has been to use legislation to protect all personal data, irrespective of its source.[81]

The Adequacy Decision provides insight into the level of legal reform states seeking reciprocity agreements will have to undertake. South Korea has been conducting reforms to its privacy laws as a part of its ongoing adequacy negotiations with the EU,[82] and India has also

---

76. *Supplementary Rules Under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU Based on an Adequacy Decision*, EUROPEAN COMM'N, https://ec.europa.eu/info/sites/info/files/annex_i_supplementary_rules_en.pdf [https://perma.cc/TB7V-D2JH]. Japan made other commitments to the EU, including "assurances to the Commission regarding safeguards concerning the access of Japanese public authorities for criminal law enforcement and national security purposes, ensuring that any such use of personal data would be limited to what is necessary and proportionate and subject to independent oversight and effective redress measures." European Commission Adopts, *supra* note 71, at 1 (emphasis omitted). The Japanese government also instituted a new "complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities," which is "administered and supervised by the Japanese independent data protection authority." *Id.* (emphasis omitted).

77. Opinion of the Board, *supra* note 17, ¶ 31 ("This framework comprises several pillars, at the centre of which there is a general statutory law, the Act on Protection of Personal Information (APPI).").

78 . YOSHIFUMI ONODERA ET AL., CHAMBERS GLOBAL PRACTICE GUIDE: DATA PROTECTION & CYBERSECURITY 4 (2d ed. 2019), http://www.mhmjapan.com/content/files/00036491/20190424-050138.pdf [https://perma.cc/MF8E-VY59].

79. *See* Opinion of the Board, *supra* note 17, ¶ 9.

80. *Id.*

81. *See* Graham Greenleaf, *Japan and Korea: Different Paths to EU Adequacy*, 156 PRIVACY LS. & BUS. INT'L REP. 9, 11 (2018).

82. Daniel R. Stoller, *South Korea Privacy Law Changes May Help EU Data Transfer Talks*, BLOOMBERG L. (Feb. 22, 2019, 11:39 AM), https://news.bloomberglaw.com/privacy-and-data-security/south-korea-privacy-law-changes-may-help-eu-data-transfer-talks [https://perma.cc/9YKM-JWV6]; *see also* European Commission Press Statement STATEMENT/17/4739, Press Statement by Commissioner Věra Jourová, Mr. Lee Hyoseong, Chairman of the Korea Communications Commission and Mr. Jeong Hyun-cheol, Vice President of the Korea Internet & Security Agency, European Commission (Nov. 20, 2017).

expressed interest in such an agreement.[83] The United States Congress is considering a federal privacy bill,[84] and California has passed the California Consumer Privacy Act, which incorporates some provisions similar to the GDPR.[85] Other states, such as New York, have also been "expanding [their] breach notification and security safeguards requirements" and attempting to strengthen data privacy legislation.[86]

The potential economic benefits to Japan, rather than the desire to provide greater data rights protections, best explain its motivation for signing the Adequacy Decision. Shintaro Kobayashi noted that Prime Minister Abe believes the Adequacy Decision will help "revitalize the economy using personal data."[87] In addition, a Japanese data privacy expert involved in the Adequacy Decision negotiations pointed out that "many Japanese companies have headquarters and branches in the EU and also hire [local] employees, which makes it necessary for the companies to transfer their . . . data outside the EU."[88] Such companies must comply with the GDPR when they seek to transfer EU customer data to non-EU destinations.[89] Prime Minister Abe's Davos speech emphasized urgency in pursuing global data governance, claiming that a data-driven economy will bring about "Society 5.0," which would benefit individuals by creating a "Data Free Flow with Trust."[90] Abe argued that "it is no longer capital but data that connects and drives everything," and that a data-driven global regime would not only benefit industry, but also reduce social inequality.[91]

The Adequacy Decision's significance for bilateral EU-Japan trade is reflected in its relationship with the EU-Japan Economic Partnership

---

83. *See* Megha Mandavia, *India to Approach the EU Seeking "Adequacy" Status with the GDPR*, ETTECH (July 30, 2019, 6:30 AM), https://tech.economictimes.indiatimes.com/news/internet/india-to-approach-the-eu-seeking-adequacy-status-with-the-general-data-protection-regulation/70440103 [https://perma.cc/H7EZ-DAKL].

84. *See* Emily Birnbaum, *Senators Inch Forward on Federal Privacy Bill*, THE HILL (Dec. 4, 2019, 4:44 PM), https://thehill.com/policy/technology/473071-senators-inch-forward-on-federal-privacy-bill [https://perma.cc/B72H-8PQY].

85. *See* Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill [https://perma.cc/V2GK-S2N5].

86. *See* Data Privacy Grp., Ropes & Gray LLP, *New York Updates Privacy Laws*, MONDAQ (Aug. 26, 2019), http://www.mondaq.com/unitedstates/x/840424/Data+Protection+Privacy/New+York+Updates+Privacy+Laws [https://perma.cc/EGQ9-YLP3] (discussing passage of New York's SHIELD Act and Identity Theft and Mitigation Services Act); *see also* Lucas Ropek, *NY's Data Privacy Bill Failed; Is There Hope Next Session?*, GOV'T TECH. (July 15, 2019), https://www.govtech.com/policy/NYs-Data-Privacy-Bill-Failed-Is-There-Hope-Next-Session.html [https://perma.cc/3J7V-PAHC] (discussing rejection of omnibus data privacy legislation).

87. Interview with Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., in Tokyo, Japan (Jan. 16, 2019) [hereinafter Kobayashi Interview].

88. Interview with Expert A, in Tokyo, Japan (Jan. 17, 2019).

89. *Id.*

90. Abe, *supra* note 2.

91. *Id.*

Agreement ("EPA").[92] The press release announcing the Adequacy Decision's adoption explicitly stated that "[t]he adequacy decisions also complement the EU-Japan Economic Partnership Decision — which will enter into force in February 2019."[93] It touted the economic benefits of the Adequacy Decision for Europe, as businesses "[would] benefit from free data flows with a key commercial partner, as well as from privileged access to the 127 million Japanese consumers."[94] Both "[t]he EU and Japan affirm[ed] that, in the digital era, promoting high privacy and personal data protection standards and facilitating international trade must and can go hand in hand."[95] An expert involved in the adequacy negotiations argued that though "some will criticize the fact that negotiations between the EU-Japan for the EPA and the adequacy assessment occurred at the same time . . . the EU and Japan have a very strong relationship and the Japanese negotiation was against the background of such economic power."[96] By "align[ing] their normative approaches to both trade and data protection," Schwartz claims that the EU and Japan "demonstrate a new model for reconciling international trade law and data protection law" and that "[d]ata protection is an essential element of international business."[97]

C. The Personal Information Protection Commission Guidelines

The controversy over the PPC Guidelines' enforceability that arose during the EU-Japan negotiations resulted from differences in the EU and Japan's political and legal systems. As described in the Adequacy Decision, the 2017 legal reform of the APPI authorized the PPC to issue guidelines that articulate "the proper and effective implementation of action to be taken by a business operator" under the data protection rules.[98] According to a data privacy expert, the use of the word "Guidelines" to describe the new legal regime became "one of the most difficult problems" during negotiations.[99]

---

92. Key Elements, *supra* note 50.

93. European Commission Adopts, *supra* note 71.

94. *Id.*

95. *Id.*

96. Interview with Expert A, *supra* note 88.

97. Schwartz, *supra* note 16, at 791–92.

98. Commission Implementing Decision, *supra* note 10, ¶ 16. The Adequacy Decision also references the seminal "Juki-Net" case in Japan. *Id.* ¶ 8. On March 6, 2018, "the [Japanese] Supreme Court held that 'citizens' liberty in private life shall be protected against the exercise of public authority, and . . . every individual has the liberty of protecting his/her own personal information from being disclosed to a third party or being made public without good reason." *Id.*

99. Interview with Expert B, in Tokyo, Japan (Jan. 17, 2019).

The Guidelines currently use a multi-step system to compel Japanese businesses to comply with regulations. The Guidelines are considered to be the "main enforcement" mechanism of the PPC.[100] Under Article 41, the Commission issues recommendations and gives businesses time to respond by making necessary adjustments.[101] The PPC can also issue orders instructing business operators that ignore its recommendations to comply.[102] A personal-information-handling business operator who violates a PPC order could potentially be "punished by imprisonment with labor for not more than six months or a fine of not more than 300,000 yen."[103] However, the APPI does not impose administrative fines on violators, and permits criminal sanctions only if all other avenues have been exhausted.[104] Furthermore, the Act only permits criminal sanctions in very specific cases, such as "if the Handling Operator refuses to co-operate with . . . an investigation by the PPC, or violates any order given by the PPC as a part of an administrative sanction."[105] Consumers can also sue business operators in tort, claiming that the latter were negligent in their information management.[106] The APPI does not provide a "definition of 'injury' or 'harm' . . . [h]owever, an infringement of privacy is a tort under the Civil Code if an individual suffers from mental burden or mental uneasiness regarding the disclosure of such information."[107] Under Japanese administrative law, companies can also appeal to the courts if they wish to dispute a PPC order.[108]

The main source of the confusion stems from the difference between Western and Japanese perspectives on the enforceability of "guidelines." In the West, the common, colloquial understanding of "guidelines" is that they "are just guidelines, they are not mandated" or

---

100. Interview with Yoichiro Itakura, Partner, Hikari Sogoh Law Offices, in Tokyo, Japan (Jan. 21, 2019) [hereinafter Itakura Interview]; *see also* ONODERA ET AL., *supra* note 78, at 5; *see also* Greenleaf & Shimpo, *supra* note 19, at 141–42 ("Most important in practice [out of the legislative elements in the Japanese government] are the Guidelines set by each Ministry.").

101. Interview with Kaori Ishii, Associate Professor, Univ. of Tsukuba, in Tokyo, Japan (Jan. 18, 2019) [hereinafter Ishii Interview]; *see also* ONODERA ET AL., *supra* note 78, at 4–5.

102. Amended APPI, art. 42; *see also* Ishii Interview, *supra* note 101.

103. Amended APPI, art. 84; *see also* Email from Kaori Ishii, Professor, Chuo Univ., to author (Jan. 20, 2020, 9:51 AM) (on file with author). The PPC is not able to impose criminal sanctions, as "[o]nly a prosecutor from the Ministry of Justice is authorized to file a criminal suit against a perpetrator." Email from Kaori Ishii, Professor, Chuo Univ., to author (Mar. 24, 2020, 8:14 AM) (on file with author).

104. *Cf.* ONODERA ET AL., *supra* note 78, at 5.

105. *Id.*

106. Ishii Interview, *supra* note 101.

107. ONODERA ET AL., *supra* note 78, at 8.

108. *See* Email from Kaori Ishii, Professor, Chuo Univ., to author (Nov. 24, 2020, 1:04 AM) (on file with author); email from Kaori Ishii, Professor, Chuo Univ., to author (Mar. 24, 2020, 8:30 AM) (on file with author).

binding on businesses or individuals.[109] However, "the APPI empowers the PPC" to adopt Guidelines, which are considered to be binding when they say that a business "must" or "should not" carry out an objective.[110] Under the APPI, "non-compliance with the relevant provisions amounts to a violation of the law."[111] Contrary to the Western concept of guidelines as non-binding, Kobayashi suggests that companies will voluntarily comply with minister-issued guidelines, "even if there is no law to prohibit such private activities."[112] This is because guidelines play a unique and important role in the Japanese regulatory framework and are an "instrument defined in the Japanese Act of Administrative Procedure."[113] Administrative guidelines allow the Japanese government to have flexibility, as ministries will issue guidelines when there are no laws on a particular matter.[114] The PPC noted that it currently utilizes the guidance system, as "the cost of losing consumers' trust is significant for companies."[115] According to the PPC, interviews with the business community provided evidence that "business operators comply with the APPI and careful consideration is required for reinforcing penalties."[116]

Despite initial concerns that the Guidelines lack enough force, the European Commission appears to have accepted the PPC's explanation that the Guidelines have been treated as effectively binding by Japanese courts, as they decided to include its language in the Adequacy Decision.[117] The Adequacy Decision points out that reforms of the APPI

---

109. Interview with Fumio Shimpo, Professor, Keio Univ., and Comm'r for Int'l Acad. Exch., Pers. Info. Protection Comm'n in Tokyo, Japan (Jan. 17, 2019) (comments were made solely in interviewee's capacity as a Professor, and not as a Commissioner) [hereinafter Shimpo Interview]. "For some industrial sectors, the ministry with jurisdiction over them has published data protection guidelines for those sectors. . . . [T]he Ministry of Internal Affairs and Communications (MIC) has issued data protection guidelines for telecommunication business operators." ONODERA ET AL., *supra* note 78, at 4.

110. Commission Implementing Decision, *supra* note 10, ¶ 16.

111. *Id.*

112. Kobayashi Interview, *supra* note 87.

113. Email from Frederike Zufall, Senior and Postdoctoral Researcher, Law, Sci., Tech. & Soc. Research Grp. at Free Univ. Brussels, to author (Jan. 19, 2020, 6:16 PM) (on file with author); *see also* Interview with Frederike Zufall, Assistant Professor, Waseda Univ., in Tokyo, Japan (Jan. 21, 2019) [hereinafter Zufall Interview].

114. *See* Shimpo Interview, *supra* note 109; *cf.* ONODERA ET AL., *supra* note 78, at 4.

115 . PERS. INFO. PROTECTION COMM'N, ACT ON THE PROTECTION OF PERSONAL INFORMATION "THE EVERY-THREE-YEAR REVIEW" OUTLINE OF THE SYSTEM REFORM 30 (2019) [hereinafter EVERY-THREE-YEAR REVIEW]. The PPC acknowledged that "revision on the current statutory penalties will be made as necessary, including introduction of a system to impose severer punishments on legal entities" in response to violations of the handling of personal information. *Id.* at 33. The PPC cautioned that though "reinforcement of penalties is a major trend . . . national legal structures and approaches to penalties differ depending on countries. Therefore, the PPC has been discussing what is preferable for Japan, taking into consideration the country's actual circumstances and legal structures." *Id.* at 32.

116. *Id.*

117. Commission Implementing Decision, *supra* note 10, ¶ 16.

strengthened the PPC's enforcement powers by consolidating the ministerial scheme under the PPC itself.[118] The Commission noted that "Japanese courts base their interpretation on the Guidelines when applying the APPI/PPC Rules in individual cases brought before them and have thus directly referred to the text of the PPC Guidelines in their judgments."[119] The Adequacy Decision also stipulates that the PPC will consider business operators' non-compliance with the Guidelines a legal violation.[120]

However, individuals affected by a violation of the Guidelines must wait to receive a remedy because companies receive multiple opportunities to respond to PPC criticism.[121] The multi-step process allows a company to redress the issue internally, rather than risk losing social reputation from a government announcement of punitive action. Japanese attorney Yoichiro Itakura states that, though companies view the PPC as an enforcement body, they also consider their relationship with the latter to be a business partnership.[122] Businesses regularly consult with the PPC and "think that they have a good relationship."[123] Additionally, following the 2020 proposed revisions of the APPI,[124] the PPC launched a new "PPC Business Support Desk" ("Support Desk") for companies on April 1, 2020, indicating a desire to promote a closer relationship with the business community.[125] The Support Desk advises corporations on personal information law via a dedicated hotline, and if necessary, provides in-person consultations.[126] Therefore, the Guidelines and Support Desk reflect the collaborative stance taken between the PPC and the Japanese business community. By contrast, European

---

118. *See id.* In addition, drawing from "information received from the PPC, those Guidelines form an integral part of the legal framework, to be read together with the text of the APPI, the Cabinet Order, the PPC Rules and a set of Q&A prepared by PPC." *Id.* (footnote omitted).

119. *Id.* at 4 n.15. The Commission further noted that the "PPC is not aware that the Court has ever diverged from the Guidelines." *Id.* The PPC had "referred the Commission to a judgment in the area of data protection where the court explicitly based itself on guidelines for its findings." *Id*.

120. *Id.* ¶ 16.

121. *See* Email from Kaori Ishii, Professor, Chuo Univ., to author (Nov. 24, 2020, 1:04 AM), *supra* note 108; email from Kaori Ishii, Professor, Chuo Univ., to author (Mar. 24, 2020, 8:30 AM), *supra* note 108.

122. Itakura Interview, *supra* note 100.

123. *Id.*

124. EVERY-THREE-YEAR REVIEW, *supra* note 115, at 30.

125. Email from Yoichiro Itakura, Partner, Hikari Sogoh Law Offices, to author (April 26, 2020, 9:43 PM) (on file with author); *see also* PERS. INFO. PROTECTION COMM'N, *PPC Business Support Desk (Reservation Required)*, https://www.ppc.go.jp/personalinfo/business_support [https://perma.cc/2H2R-53XV] [hereinafter *Support Desk*]; *see also* EVERY-THREE-YEAR REVIEW, *supra* note 115, at 30.]; PERS. INFO. PROTECTION COMM'N, *Establishment of PPC Business Support Desk* (Mar. 23, 2020) https://www.ppc.go.jp/files/pdf/20200323_houdou.pdf [https://perma.cc/T4TZ-XKFS]; Email from Yoichiro Itakura, Partner, Hikari Sogoh Law Offices, to author (Jan. 19, 2020, 7:18 PM) (on file with author).

126. *See Support Desk*, *supra* note 125.

data protection authorities have a relationship with European businesses focused around punitive actions.[127]

Pointing to the lack of punitive measures, scholars such as Frederike Zufall criticize Japan for not having strong enough data enforcement powers.[128] Others, like Professors Greenleaf and Shimpo, argue that "[s]trong yet unsubstantiated claims are made by government bodies and academics that Japanese businesses comply with the legislation" due to soft power mechanisms.[129] However, Greenleaf and Shimpo point out that the unsubstantiated nature of these claims may in itself be a deficiency.[130] Conversely, Professor Hiroshi Miyashita claims that "soft power mechanisms for enforcing protection of personal information has been functioning well in the context of Japanese social norms and cultural values."[131] He argues that the lack of sanctions is not always a negative, and may actually be an indication of the system's success.[132]

Due to criticisms from the EDPB, the independent European body that advises the European Commission on data-related legislation,[133] the following round of negotiations will likely focus on the APPI Guidelines' enforceability. The EDPB acknowledged that "[a]ccording to the PPC, the Guidelines are followed in practice nevertheless as it is local custom."[134] However, the EDPB asked for further information and monitoring to demonstrate "that the Guidelines are legally binding norms."[135] In particular, the EDPB requested further clarification regarding the PPC's assertion that "the Japanese courts use the PPC Guidelines to render their judgments when applying APPI rules."[136] Such revisions will likely take place during the next periodic review of the Adequacy Decision, as the European Commission adopted it in January 2019 without addressing the Board's critiques of the December 2018 Adequacy Decision draft.

---

127. *See infra* Part IV.

128. *See* Zufall Interview, *supra* note 113.

129. *See* Greenleaf & Shimpo, *supra* note 19, at 139.

130. *Id.*

131. Hiroshi Miyashita, *A Tale of Two Privacies: Enforcing Privacy with Hard Power and Soft Power in Japan*, *in* ENFORCING PRIVACY 105, 116 (David Wright & Paul de Hert eds. 2016).

132. *Id.*

133. *About EDPB*, EUROPEAN DATA PROT. BD., https://edpb.europa.eu/about-edpb/about-edpb_en [https://perma.cc/9PEP-S6AD].

134. *See* Opinion of the Board, *supra* note 17, ¶ 54.

135. *Id.* ¶ 48–54.

136. *Id.* ¶ 54. In particular, the Board referenced the 2006 court ruling "to provide evidence that the Japanese courts base themselves on guidelines for their findings." *Id.* Stating that "the EDPB was not provided with this court ruling," the Board asked if the "European Commission could provide, if available, a more recent court ruling, either in the field of data protection or in another sector where the Japanese courts have used the PPC Guidelines or other similar guidelines as a basis of their decision." *Id.*

IV. CULTURAL ENFORCEMENT MECHANISMS IN THE AGE OF GLOBALIZATION

Europe and Japan have very different concepts of enforcement, as the former primarily operates through punitive action ("hard power") as compared to the latter which mostly operates through reputation ("soft power"). Professor Miyashita suggests that European data protection regimes incentivize companies to enforce privacy through a "hard power" perspective, such as a powerful regulatory body, law enforcement, and punishment.[137] Conversely, "soft power" coerces companies to enforce privacy through "cultural value and social norms."[138] Under this type of data governance, "[a] data protection authority may assist in the promotion of a privacy culture through soft enforcement."[139] He argues that such soft power mechanisms "ha[ve] worked to some extent" in Japan.[140] He claims that "businesses generally follow guidelines issued by government ministries" due to fear of violating social norms.[141] According to Professor Miyashita, "the risk of loss of social trust and business reputation [from a data breach] is regarded as much more significant than paying a fine."[142] Though he does not prioritize one type of power over the other, he suggests that "enforcing privacy may be more effective if both hard and soft powers are used."[143]

Interviewees generally agreed that reputational value serves as an important enforcement mechanism in Japan, particularly for data breaches. Though Professor Shimpo, Professor Taro Komukai, and Kobayashi rejected the wholesale application of the "hard power" versus "soft power" framework, these experts agreed that cultural values compel compliance with the Guidelines.[144] Professor Shimpo stated that "in Japan, we do not use the word soft power."[145] However, he also suggested that the cultural differences between the concepts of hard power and soft power are similar to the disparities between law and the PPC Guidelines.[146] Professor Komukai agreed that "in Japan, reputation and

137. *See* Miyashita, *supra* note 131, at 108.

138. *Id.* at 106.

139. *Id.* at 108.

140. *Id.* at 106.

141. Miyashita, *supra* note 19, at 233.

142. *Id.*

143. Miyashita, *supra* note 131, at 106. Miyashita states that "it is wrong to simply label the European approach as hard power enforcement and Japanese approach as soft power enforcement. . . . The enforcement of privacy is dependent on the choice of societal and cultural values." *Id.* at 120.

144. *See* Shimpo Interview, *supra* note 109; *see also* Kobayashi Interview, *supra* note 87; Interview with Taro Komukai, Professor, Nihon Univ., in Tokyo, Japan (Jan. 21, 2019) [hereinafter Komukai Interview].

145. Shimpo Interview, *supra* note 109.

146. *See id.*

social pressure have greater meaning" than in the EU.[147] However, he emphasized that the "Japanese discussion associated with data protection has been and is very focused on data leakage or third-party provisions."[148] The reputational and social ramifications of a data breach would lead to a loss of consumer trust, a decrease in the company's market value, and a harm to workers.[149] Due to these consequences, Kobayashi agreed that the PPC "does not have to use a large number of fines" in order to compel compliance with the APPI Guidelines or other regulations.[150] This perspective is consistent with the Japanese view that the PPC Guidelines allow social costs to effectively enforce the rules on businesses.

One example of a Japanese company proactively apologizing to the public in response to a data breach is the seminal Benesse case. Numerous experts cited a data leak which "affected approximately 48.6 million people in Japan (approximately one third of the country's total population),"[151] as a landmark case.[152] The Japanese company Benesse voluntarily provided each affected victim with a 500 yen coupon (around USD $4), and publicly apologized.[153] In response to what was billed as a "symbolic" gesture, "a limited number of people wanted legal action," and instead "most people accepted the 500 yen coupon."[154]

147. Komukai Interview, *supra* note 144.

148. *Id.*

149. *See id.*

150. Kobayashi Interview, *supra* note 87.

151. *Largest Multi-Plaintiff Action Ever in Japan Over Data Breach*, WINSTON & STRAWN LLP (Feb. 5, 2015), https://www.winston.com/en/privacy-law-corner/largest-multi-plaintiff-action-ever-in-japan-over-data-breach.html [https://perma.cc/GRW2-BEJN]; *see also Customer Data Leak Deals Blow to Benesse*, NIKKEI ASIAN REV. (July 10, 2014, 6:00 AM), https://asia.nikkei.com/Business/Customer-data-leak-deals-blow-to-Benesse [https://perma.cc/27GT-JW6G].

152. *See* Ishii Interview, *supra* note 101; *see also* Kobayashi Interview, *supra* note 87; Komukai Interview, *supra* note 144; Murata Interview, *supra* note 65.

153. *See Customer Data Leak Deals Blow to Benesse*, *supra* note 151; *Largest Multi-Plaintiff Action Ever in Japan Over Data Breach*, *supra* note 151.

154. *See* Kobayashi Interview, *supra* note 87. Numerous people filed multi-plaintiff civil claims after receiving the 500 yen coupon, and some of the affected individuals have filed claims against the company. *Largest Multi-Plaintiff Action Ever in Japan Over Data Breach*, *supra* note 151. "By the end of January 2015, 1,789 complaints had been reported, but according to the lawyers, over 1,000 further plaintiffs are expected to file claims during February. . . . Unlike class actions in the U.S., multi-plaintiff actions in Japan commence with individual claims from each plaintiff." *Id.* "Benesse originally offered compensation of $4 per person, although the claims filed ask for much higher amounts, ranging from the equivalent of $125 to over $850 for the harm caused by the data breach." *Id.* The Tokyo high court decision ordered Benesse to pay a 2,000 yen penalty per person on the grounds that the data breach caused emotional distress to victims. *See* Eri Shinya (新屋絵理), *Zyouhou Ryuushutsu, Benetto No Baisyou Sekinin Mitomeru Hazime No Hanketsu Tokyo Kousai* (情報流出、ベネッセの賠償責任認める初の判決　東京高裁) [*Tokyo High Court Rules That Education Company Benesse Corporation has Legal Liability in First Ever Finding That a Party Must Provide Compensation to Customers for Data Breach*], ASAHI SHIMBUN DIGITAL (June 28, 2019, 8:46 PM), https://www.asahi.com/articles/ASM6X64WWM6XUTIL043.html [https://perma.cc/2YXW-2TKN]. In a separate

As described by Kobayashi, Benesse's behavior aligned with conventional Japanese business practices.[155]

Data privacy experts have also emphasized the importance of a company publicly apologizing in the wake of a data breach in Japan. According to Professor Komukai, Japanese companies are willing to proactively address data breaches, because the public views a data breach as the company "breaking the trust of the public," and committing an act "against their expectations."[156] Such feelings of trust are more important than "actual [monetary] damages."[157] Professor Shizuo Fujiwara stated that the monetary value provided to data breach victims in compensation is less important than the apology from the company.[158] He suggested that this might be due to "shame culture" which emphasizes the significance of community reputation in Japan.[159] Furthermore, Professor Kaori Ishii described how the apology can take the form of a public press conference.[160] At such a conference, the company's leadership could take responsibility for the breach in various ways, with one prominent example being bowing and apologizing to the public.[161]

However, tension arises when multinational companies operating in Japan do not share the same cultural norms as domestic businesses. Such international corporations benefit from access to the Japanese market and personal data. Even so, they typically do not take proactive steps in response to data breaches in accordance with domestic cultural norms. The following two case studies explore this phenomenon: (1) Google's streamlining of privacy policies in 2012, and (2) the Cambridge Analytica scandal.

First, both the EU's and Japan's responses after Google streamlined privacy policies across services in 2012 illustrates the differences in enforcement action and punitive power between the data regimes. The multinational company announced that all privacy policies across

---

lawsuit, the Osaka High Court found that Benesse must provide 1000 yen compensation to victims of the data breach. *See Kokyakuzyouhouryuu Shutsu, Benetto Ni Sen En Baisyou Meirei* [*Osaka Court Finds That Company Must Provide 1000 Yen Compensation*], SANKEI WEST (Nov. 20, 2019, 5:16 PM), https://www.sankei.com/west/news/191120/wst1911200028-n1.html [https://perma.cc/8RXH-W369].

155. *See* Kobayashi Interview, *supra* note 87.

156. Komukai Interview, *supra* note 144.

157. *Id.*

158. *See* Interview with Shizuo Fujiwara, Professor, Chuo Law Sch., and Comm'r, Pers. Info. Protection Comm'n in Tokyo, Japan (Jan. 17, 2019) [hereinafter Fujiwara Interview] (making comments solely in interviewee's capacity as a Professor and not as a Commissioner).

159. *Id.*

160. *See* Ishii Interview, *supra* note 101.

161. *See id.*

Google services would be integrated into one document.[162] The French data protection authority subsequently fined the company 50 million euros for violating the GDPR.[163] In contrast, Japan "only warned" Google after the announcement, "and the warning was almost ignored."[164]

Second, the PPC's landmark warning to Facebook in 2018 in response to the Cambridge Analytica scandal raised significant questions about Japan's ability to protect consumers when dealing with a foreign company. The Cambridge Analytica affair involved a political consulting firm whose data leak of Facebook users' data "ha[d] been used by US President Donald Trump's election campaign body in 2016."[165] The data breach potentially impacted over 100,000 Japanese Facebook users.[166] The Commission instructed Facebook "to improve its protection of personal information," and found that the company's "management of personal information and its explanation to its users were inappropriate."[167] The PPC "demand[ed] that Facebook respond appropriately to the problem, including communicating sufficiently with the users and deleting data as necessary."[168] Facebook apparently did not violate any Japanese laws in the Cambridge Analytica scandal, as the breach "occurred prior to the enforcement of the revised Japanese data protection law."[169] However, the Commission's instructions to the social media giant are "regarded as a landmark action in Japan,"[170] as the warning was "the first extraterritorial application of the APPI."[171]

In comparison, the PPC's order seems to have been insufficient to compel Facebook to act in accordance with Japanese cultural practices. The lack of financial penalties levied by the Japanese authorities starkly

---

162. *See* Tim Carmody, *Google Streamlines Privacy Policy to Integrate Its Products*, WIRED (Jan. 24, 2012, 6:16 PM), https://www.wired.com/2012/01/google-streamlines-privacy [https://perma.cc/7TWZ-ZH62].

163. *See The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against Google LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc [https://perma.cc/S5PY-EMM7].

164. Email from Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., to author (Aug. 22, 2019, 7:06 AM) (on file with author). "At the time, the PPC had yet to be established, so the authority in charge was the Ministry of Economy, Trade and Industry (METI) and Ministry of Internal Affairs and Communications (MIC)." *Id.*

165. Associated Press, *Japan to Order Facebook to Improve Data Protection After Mass Cambridge Analytica Leak*, SOUTH CHINA MORNING POST (Oct. 22, 2018, 1:38 PM), https://www.scmp.com/news/asia/east-asia/article/2169627/japan-order-facebook-improve-data-protection-after-mass [https://perma.cc/J3U7-56QU].

166. *See id.* Furthermore, the Commission also instructed the social media giant to conduct a probe into a separate data breach in September 2018 that affected 29 million accounts. *See id.*

167. *Id.*

168. *Id*.

169. Shimpo Interview, *supra* note 109.

170. *Id.*

171. Kobayashi Interview, *supra* note 87.

contrasts with the USD $5 billion fine levied by the U.S. Federal Trade Commission[172] and the rumors of an impending fine exceeding 1 billion euros that could be imposed by Ireland's Data Protection Commission, which has been spearheading the EU's investigation.[173] In contrast, the PPC's instructions "carrie[d] no administrative orders or penalties and [were] not legally binding."[174] Facebook did respond by "promis[ing] to detail on its Japanese-language website how it will address the request."[175] Yet, Kobayashi criticized the company for not "expressing enough apology for Japanese users as Japanese firms usually do."[176] According to Kobayashi, "a Japanese company would seriously reflect" and communicate "what measures they [would] do next if they receive a warning or administrative guidance" from the PPC, even if the warning was legally non-binding.[177] Additionally, a Japanese corporation "would express public apology and even might pay a small amount" to each victim of the data breach as an expression of contrition.[178] Facebook has yet to take such steps to communicate what measures it will take in response to the PPC's instructions.

These two examples illustrate the limitations of soft power cultural mechanisms as an effective means of enforcement against multinational companies operating in Japan. Though Facebook took more action than Google in response to the government's warnings, neither corporation acted in accordance with Japanese cultural practices on par with a Japanese company such as Benesse. Professor Fujiwara stated that "soft laws may not be applicable for foreign companies located in Japan," as "culture is not easily changed."[179] Similarly, Professor Komukai expressed concern that cultural enforcement mechanisms do not affect international companies.[180] Such businesses might not understand or care to abide by the same cultural norms as Japanese companies, because they do not prioritize public opinion in Japan to the same degree as a domestic company.[181] He stated that "Japanese people think

172. *See* Cecilia Kang, *F.T.C. Approves Facebook Fine of About $5 Billion*, N.Y. TIMES (July 12, 2019), https://nyti.ms/2XHcVc4 [https://perma.cc/Q62X-96DV].

173. *See* Emily Price, *The EU Could Hit Facebook with Billions in Fines over Privacy Violations*, DIGITAL TRENDS (Aug. 12, 2019, 10:55 AM), https://www.digitaltrends.com/social-media/facebook-gdpr-decision [https://perma.cc/CG9T-SZA5].

174. Makiko Yamazaki, *Japan Tells Facebook to Improve Data Protection*, REUTERS (Oct. 21, 2018, 11:25 PM), https://www.reuters.com/article/us-facebook-privacy-japan/japan-tells-facebook-to-improve-data-protection-idUSKCN1MW0AG [https://perma.cc/XS6W-2JS3].

175. *Id.*

176. Email from Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., to author (Aug. 21, 2019, 7:10 AM) (on file with author).

177. *Id.*

178. *Id.*

179. Fujiwara Interview, *supra* note 158.

180. *See* Komukai Interview, *supra* note 144.

181. *See id.*

that they can ask Benesse to do something for them, but they don't think" that they have the same level of control over Facebook's actions.[182]

Japan seems to be taking steps to address the heightening tension between global companies operating within Japan and the local cultural enforcement framework by strengthening the APPI's extraterritorial application. Instead of waiting for multinational businesses to conform to Japanese culture, the government is proactively proposing to grant the PPC stronger punitive enforcement powers against the corporations themselves.[183] The 2020 Cabinet Decision on the Amendment Bill of the APPI ("Cabinet Decision") suggested bolstering the PPC's enforcement powers against foreign business operators.[184] Under the current version of the APPI, the PPC is not permitted to collect reports, conduct onsite inspections, or issue orders to foreign companies.[185] Rather, the PPC issues "guidance, advice, or recommendations" to foreign businesses.[186] It can then "request a foreign authority that enforces a foreign law equivalent to the APPI to cooperate in taking measures based on the foreign law" if the company fails to comply.[187] In response to the rising number of data leakage incidents as well as PPC guidance and advice on matters involving foreign business operators, the PPC acknowledges the criticism that "the situation is problematic in terms of fairness between domestic [and foreign] business operators."[188] In order to mitigate this problem, proposed amendments include allowing the PPC to publicize a foreign company's failure to follow an order, and for the first time, to conduct "onsite inspection of a foreign business operator." [189] The Cabinet Decision also recommended reforming the APPI to grant the PPC the authority to "collect[ ] reports and orders, which are enforced with a penalty" against foreign business operators.[190]

---

182. *Id.*

183. *See Japan's Info Protection Panel Considers Beefing Up Protections for Internet Users' Data*, JAPAN TIMES (Apr. 25, 2019), https://www.japantimes.co.jp/news/2019/04/25/business/japans-info-protection-panel-considers-beefing-protections-internet-users-data/ [https://perma.cc/HC73-4PTY] [hereinafter *Japan's Info Protection Panel]*.

184. PERS. INFO. PROTECTION COMM'N, *The Amendment Bill of the Act on the Protection of Personal Information, etc. (Overview)* (2020), https://www.ppc.go.jp/files/pdf/amendment_bill202003.pdf [https://perma.cc/3L3G-NHTV] [hereinafter *Cabinet Decision*]. A foreign personal handling business operator ("PIHBO") falls under the APPI's purview if it "handles personal information or anonymously processed information produced by using the personal information when (1) the PIHBO supplies a good or service to a person in Japan and (2) the PHIBO acquires personal information of the person." EVERY-THREE-YEAR REVIEW, *supra* note 115, at 34.

185. EVERY-THREE-YEAR REVIEW, *supra* note 115, at 34–35.

186. *Id*. at 34–35.

187. *Id*. at 34–35.

188. *Id*. at 35.

189. *Id*. at 34–35.

190. *Cabinet Decision*, *supra* note 184.

Moreover, Japan seems to be addressing these issues of extraterritoriality by broadening the scope of personal rights under the APPI. In 2019, the PPC suggested revising the APPI to "expand the scope of personal rights" to "requir[e] companies to stop using personal information for such purposes as advertising if requested by consumers."[191] This amendment would compel businesses to "remove personal data" on a mandatory, rather than "voluntary basis."[192] In addition, these proposed changes specifically address both domestic and international companies, such as Google and Amazon, which are located outside Japan.[193] In 2020, the Cabinet Decision proposed expanding the scope of individual rights under the APPI by relaxing "requirements for the cease of utilization [as well as deletion, and cease of provision to a third party] . . . in cases in which there is a possibility of violating individual rights or legitimate interests."[194] However, these "stronger individual request rights on suspension of use and erasure" under an amended APPI will only apply if there likely will be harm to an "individual's legitimate interest," and the PPC has yet to release guidance classifying advertising under such "harmful cases."[195] As the Cabinet Decision was approved and submitted to the National Diet of Japan on March 10, 2020 as part of the PPC's "Every-Three-Year Review" of the APPI, such major amendments and PPC guidance could come into effect in the near future.[196] Furthermore, the PPC has been considering whether or not to include a European-style "right to be forgotten" in the APPI.[197] Such developments would ensure that the APPI move closer to the rights enshrined in the European Charter.

Current plans to address this problem by strengthening the authority of the Japan Fair Trade Commission ("JFTC") also suggest that the

---

191. *Japan's Info Protection Panel*, *supra* note 183.

192. *Id.*

193. *See id.*

194. PERS. INFO. PROTECTION COMM'N, *"The Every-Three-Year Review" of the Act on the Protection of Personal Information Outline of the System Reform (Main Points)* https://www.ppc.go.jp/files/pdf/The_Every_Three_Year_Review_of_the_APPI_Outline_of_the_System_Reform_main_points.pdf [https://perma.cc/AF8P-NE64]; *see also* PERS. INFO. PROTECTION COMM'N, *Act on the Protection of Personal Information "The Every-Three Year Review" Outline of the System Reform,* https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20200124 [https://perma.cc/6QZT-LPTD]; EVERY-THREE-YEAR REVIEW, *supra* note 115 at 9-10; PERS. INFO. PROTECTION COMM'N, *Cabinet Decision on the Amendment Bill of the Act on the Protection of Personal Information, etc.* (Mar. 24, 2020) https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20200324 [https://perma.cc/L4NF-B5XM].

195. Email from Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., to author (April 27, 2020, 7:51 PM) (on file with author).

196. *See id.* At the time of publication, proposed amendments to the APPI include strengthening the PPC's penalty mechanisms, such as "imprisonment with labor for not more than 1 year or as a fine of not more than 1 million yen" for violations of a PPC order, and "a fine of not more than 500,000 yen" for "false submissions of a report" to the PPC. *See Cabinet Decision*, *supra* note 184.

197. *Japan's Info Protection Panel*, *supra* note 183.

PPC will receive additional enforcement powers. The JFTC "has drafted guidelines stipulating that it can consider cases where information technology giants obtain personal data without consent as violations of the country's antimonopoly law."[198] This development "is aimed at preventing IT giants from obtaining and using personal information in an inappropriate manner."[199] These new powers will allow the JFTC to "issue cease-and-desist orders over cases violating the antimonopoly law and impose fines if impacts from the practices involved are serious."[200] The likelihood of Japan conducting legal reforms to strengthen the PPC's enforcement powers is further discussed in the next section.

V. JAPAN AS A NEW MODEL OF COOPERATIVE DATA PRIVACY

Rather than adopting the GDPR wholesale or rejecting the framework completely, the Japanese model of cooperative data privacy will likely limit reforms to the Adequacy Decision. In response to the EDPB's criticisms, the Adequacy Decision will be amended in 2021 and then undergo periodic review every two years.[201] Due to strong economic incentives for Japan to uphold the Adequacy Decision, it is highly probable that the country would be willing to amend the Adequacy Decision in response to the EDPB's criticisms during future rounds of revisions. An expert involved in the adequacy negotiations provided a personal opinion that the "EDPB will be considered during the process of the next amendment."[202] Professor Ishii stated that Japan would likely "have to abide by [European] requests" to maintain the

198. *Japanese Antimonopoly Watchdog Drafts Guidelines to Regulate IT Giants*, JAPAN TIMES (July 17, 2019), https://www.japantimes.co.jp/news/2019/07/17/business/japanese-antimonopoly-watchdog-drafts-guidelines-regulate-giants [https://perma.cc/4MK5-FSQ5].

199. *Id.* Furthermore, according to Kobayashi, "there is no adjustment rule between the PPC and the [J]FTC…[the] administration seeks to weaken tech giants' power by the antitrust law; however, it clearly overlaps PPC's jurisdiction" which creates uncertainty for businesses. Email from Shintaro Kobayashi, Senior Consultant, Nomura Research Inst., to author (Oct. 20, 2019, 12:27 AM) (on file with author). The "PPC insists that if a case concerns data protection issues, it will judge by itself, or at least in cooperation with [J]FTC." *Id.* The PPC has issued a statement in response to JFTC's initiative. *See* Press Release, Pers. Info. Protection Comm'n, Dejitaru purattofōmā to kojin jōhō-tō o teikyō suru shōhisha to no torihiki ni okeru yūetsutekichiinoran'yō ni kansuru dokusen kinshi-hō-jō no kangaekata (an)' ni taisuru tō iinkai no kangaekata ni tsuite (「デジタル・プラットフォーマーと個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方（案）」に対する当委員会の考え方について) [Opinion of the Committee on the "Draft of Guidelines on Anti-Monopoly and Abuse of Superior Bargaining Position in Transactions Between Digital Platforms and Consumer Providers of Personal Information"] (Aug. 29, 2019), https://www.ppc.go.jp/files/pdf/190829_houdou.pdf [https://perma.cc/6U7Y-F5SD].

200. *Japanese Antimonopoly Watchdog Drafts Guidelines to Regulate IT Giants, supra* note 198.

201. *See* Shimpo Interview, *supra* note 109; *see also* Opinion of the Board, *supra* note 17, at 12; European Commission Adopts, *supra* note 71.

202. Expert B, *supra* note 99.

adequacy agreement.[203] Itakura suggested that there is external pressure from the international community on Japan to strengthen the PPC's enforcement powers.[204] Moreover, as the Board's critiques of the Adequacy Decision have primarily focused on the PPC's enforcement mechanisms, it is likely that Japan would "move closer to the GDPR" data privacy framework.[205]

Even so, numerous data privacy experts in Japan expressed concerns that importing a GDPR system wholesale into the country would be incompatible with local culture, highlighting discomfort with the Brussels Effect. As privacy is situated within the context of values and cultures,[206] importing the EU infrastructure would impose a new, Western framework on Japan. According to Professor Ishii, the general consensus within the Japanese privacy community is that an EU-style data privacy regime "would not be suitable for the country due to the cultural differences."[207] Several off-the-record interviewees stated that the overall view of the Japanese data protection community is that they do not think that the GDPR is necessarily the right system for Japan.[208] Professor Komukai theorized that this incompatibility is because of the "uniqueness of [the] Japanese legal system," and "maybe because of the cultural background or historical background" of the APPI.[209] He emphasized that while the "APPI will have more amendment[s] in the near future" which would "reflect[] the discussion with the EU and other countries," he did not "think it [would] be [a] similar legal scheme [to] the EU['s] (GDPR)."[210] Such reservations about the incompatibility between the two cultures would likely make any revisions to the Japanese privacy regime reactive and incremental.

Furthermore, the Adequacy Decision creates a two-track system for data privacy, illustrating the potential limits of the Brussels Effect. The protections for personal data transferred from the EU to Japan are protected by the APPI in conjunction with the Supplementary Rules, which grant the data a "higher level of protection than [the] Japanese APPI."[211] However, the Supplementary Rules do not protect data flows

---

203. Ishii Interview, *supra* note 101.

204. *See* Itakura Interview, *supra* note 100.

205. *See id*.

206. *Compare* GDPR *with* Amended APPI.

207. Ishii Interview, *supra* note 101.

208. *See* Interview with Experts C, D and E in Tokyo, Japan (Jan. 18, 2019) [hereinafter Experts C, D and E].

209. Komukai Interview, *supra* note 144.

210. *Id*.

211. Email from Kaori Ishii, Professor, Chuo Univ., to author (Mar. 25, 2020, 7:37 AM) (on file with author); *see also* Commission Implementing Decision, *supra* note 10, at 31; *Questions & Answers*, *supra* note 12.

from Japan to the EU, as "the provisions of Article 24 of the APPI applies and the GDPR will be applied after" the data transfer.[212] Data handled and processed within Japan (and which is excluded from the GDPR's territorial scope) is also only protected by the APPI's lower standard.[213] As a result, Japan now has a lower standard of domestic protection for personal data than for handling and processing EU data. This two-track model of data privacy can be explained by the fact that international trade served as the main driver behind the adoption of the agreement, rather than a change in the Japanese public's attitude towards stricter privacy protections.[214] "[A]n identical level of protection between [the] APPI and GDPR" is not mandated for an adequacy finding, as long as "it guarantees an [essentially equivalent] level of protection."[215] After all, as Japanese data privacy is primarily driven by business interests, rather than a fundamental rights-based framework, it is unnecessary for Japan to grant additional protections to data handled and processed domestically if there is no internal pressure.

As there is currently little incentive for Japanese businesses to provide a level of domestic protection on par with the protections given to those covered by the GDPR, the two-track system is likely to remain for the foreseeable future.[216] This regime seems to support Professor Schwartz's claim that the EU-Japan Adequacy Decision contradicts Professor Bradford's timeline as it was presented in Part II.[217] Bradford suggested that in response to a "de facto Brussels Effect," pressure from export-oriented companies on governments to change domestic regulations leads to a "de jure Brussels Effect."[218] Yet, the Japanese model indicates that Japanese legal reform will only satisfy the minimum requirements of compliance with the GDPR in a reactive manner. This dynamic suggests that although Japan has moved closer to the EU in its international data protection practices, the GDPR's effects are limited within the country. However, as big data has changed domestic culture, attitudes towards stricter privacy protections for personal data handled and processed within Japan could also potentially change to match the EU's. According to Professor Ishii, the Internet and big data has

212. Email from Fumio Shimpo, Professor, Keio Univ., and Comm'r for Int'l Acad. Exch., Pers. Info. Protection Comm'n in Tokyo, Japan to author (April 7, 2020, 12:16 PM) (making comments solely in interviewee's capacity as a Professor and not as a Commissioner) (on file with author). *See also* Amended APPI, art. 24.

213. *See* Commission Implementing Decision, *supra* note 10, ¶ 31; *see also Questions & Answers*, *supra* note 12. Article 3 of the GDPR stipulates that the Regulation applies to businesses outside of the EU if the company (1) offers goods or services to data subjects residing in the EU, or (2) if the organization monitors their online behavior. GDPR, *supra* note 11, art. 3.

214. *See* Kobayashi Interview, *supra* note 87.

215. Shimpo Email, *supra* note 212.

216. *See* Experts C, D and E, *supra* note 208.

217. *Compare* Bradford, *supra* note 18, at 6 *with* Schwartz, *supra* note 16, at 804.

218. *Id.*

"changed [Japanese] culture," particularly people's notions of privacy and data breaches.[219] Indeed, if the cost of compliance with both domestic and international regulations is too high for domestic businesses, they could still apply pressure on the government to increase domestic privacy protections to the EU's level.

The Japanese model of cooperative data privacy provides a precedent for parties seeking to benefit from the economic salience of data flows, but are concerned about the societal and cultural implications of the Brussels Effect. A reactive model allows a country to reap the financial benefits of an adequacy decision while cabining the extent of reforms to its domestic privacy framework. Instead of proactively adopting European standards, and viewing data privacy as a fundamental right, Japan is likely incentivized to only meet the minimum standard required to maintain adequacy. Rather than importing the entire EU system at once, the country will likely conduct incremental legal reforms in response to continuing pressure from the EDPB. The two-track model of data privacy that provides a lower level of protection for personal data processed and handled within Japan will likely remain. Thus, the Adequacy Decision represents not only the convergence and conflict between two privacy regimes, but also the limitations on the European vision of utilizing the GDPR to establish global human rights standards.

These limitations reflect the fact that the future of data governance is also significant for geopolitical competition. The rules of data privacy cause material consequences that reflect and implicate identity, values, and cultures. In today's world of rising technological rivalry between China and the U.S.,[220] "[t]he United States, Europe, and China have realized technology is neither culturally neutral nor devoid of values."[221] As these "embedded [values] in tech . . . fuel[] soft power" and "hard, military power,"[222] setting data governance standards has become imperative for states jockeying for position in the global arena. This dynamic has also led to concerns that the absence of an international consensus and the rise of data localization (reflected by information increasingly being "confined within national borders") could lead to "an internet fragmented as a result of different national regulations," known as a "splinternet."[223] The lack of a global baseline also provides parties with significant economic leverage, such as the EU, with a key opportunity to influence other countries' privacy regimes.

---

219. *See* Ishii Interview, *supra* note 101.

220. *See* Sacks & Sherman, *supra* note 4.

221. ANDRÉS ORTEGA, THE U.S.-CHINA RACE AND THE FATE OF TRANSATLANTIC RELATIONS 5 (2020), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/200113_USChinaTranstlanticRelations.pdf [https://perma.cc/9PP7-EQ6C].

222. *Id.*

223. Koizumi, *supra* note 9.

By extension, such countries can then impact the future of soft power, geopolitics, national security, culture, and technological innovation. Therefore, the Japanese system of cooperative data privacy can serve as an important precedent for parties seeking an alternative to the U.S., European, and Chinese data privacy models. This framework positions Japan between the EU and the U.S. models of data privacy, and other states may follow its example moving forward.[224] Thus, Japan demonstrates that there is a middle path to preserving a state's values, culture, and identity in the face of pressure from the radically changing technological landscape.

VI. CONCLUSION

Prime Minister Abe's speech at Davos urged fellow world leaders to "act now" to establish global data governance rules, "because coming into being every single day is more than 2.5 quintillion bytes of data."[225] He claimed that worldwide data regimes should balance protecting personal and sensitive data while ensuring that countries can reap the economic benefits of data flows.[226] As evidenced by Prime Minister Abe's speech, Japan seeks to benefit financially from free-flowing data by leading in the escalating competition to establish universal data governance standards. The Adequacy Decision illustrates the complexities of harmonizing two disparate data privacy regimes with differing cultures and values. The Adequacy Decision also plays an important role in global data governance, as it is the first adequacy decision signed after the GDPR came into effect, and the first mutual adequacy agreement.

Further, the Adequacy Decision represents the remarkable story of the Japanese model of cooperative data privacy. It illustrates how the EU and Japan harmonized their privacy frameworks, despite significant cultural, social, and legal challenges. Case studies of the fundamental discrepancies between the EU and Japanese perspectives of data protection illustrate the source of these disparities, and the controversy over the PPC Guidelines which arose during negotiations between the two sides can be partially explained by them. The Adequacy Decision illustrates how market forces can influence values, identities and cultures in the era of a borderless Internet. Domestic resistance within Japan to an EU-style privacy architecture and the current two-track

224. Professor Schwartz noted that Japan "has the potential to serve as . . . a model for other Asian countries deciding on a privacy regime." Schwartz, *supra* note 16 at 807. It is worth noting however that the Japanese framework is equally applicable to other nation states globally.

225. Abe, *supra* note 2.

226. *Id.*

system of data privacy illustrates the gap between a business-focused versus fundamental rights-based regime.

Rather than adopting or rejecting the GDPR in full, Japan provides an alternative regulatory option to the current U.S., European, and Chinese data privacy systems. In the absence of an international consensus, the question of which data governance model — and which values — will win in the geopolitical rivalry to control access to data is of paramount importance. The Japanese model allows a party to reap the financial benefits of an adequacy decision while cabining the extent of reforms to its domestic privacy framework and culture. Though future revisions will probably strengthen the PPC's enforcement powers, it is unlikely that Japan will move significantly closer towards an EU-style data privacy framework. Therefore, the EU-Japan Adequacy Decision not only represents a new frontier for global data governance, but also the limits of the Brussels Effect and the European vision of promulgating human rights standards worldwide through the GDPR. Japan has chartered a new path for countries seeking to implement their own data privacy reforms, and for understanding the potential ramifications of such a decision on their domestic values, culture, and identity.