THE BEST DATA PLAN IS TO HAVE A GAME PLAN: OBSTACLES AND SOLUTIONS TO REACHING INTERNATIONAL DATA PRIVACY AGREEMENTS

James Y. Wang[*]

ABSTRACT

The modern digital world relies on the instantaneous transfer of data. This digital highway is essential for the growth of the modern digital economy and contributes to the rise of globalization. In order to facilitate these data transfers, ground rules must first be put into place. To date, there are few, if any, binding international data privacy agreements. This is in part due to practical considerations, such as high administrability costs, inadequate enforcement agencies, and complex jurisdictional procedures. More fundamentally, however, this is due to competing incentive structures, as countries are incentivized to protect their own digital sovereignty by limiting the transfer of their own data, but also wish to accept the data flowing from other countries. The result is a zero-sum game between local data protectionism and free cross-border data flows. To understand how these incentive structures function and how to resolve various gridlocks, this Note delves into the Safe Harbor Agreement between the United States and the European Union and applies an analytical game theory approach to track the agreement's formation and its eventual breakdown. This Note concludes by proposing several potential solutions to overcome the obstacles preventing the successful implementation of international data privacy agreements.

[*] J.D. Candidate, 2022, University of Michigan Law School; B.A., 2017, New York University. Thank you to my friends and family for your unending love and support throughout law school. A special thank you to Abby Sun, Stephanie Lam, Kimberly Parry, Alex Theodosakis, Josh Zhao, and the Michigan Technology Law Review team for your invaluable guidance, assistance, and dedication in making this Note possible.

TABLE OF CONTENTS

INTRODUCTION

The modern digital world has made the world smaller and faster, with information and data transferred within an instant and ignoring all physical borders. This "digital highway" is essential for much of our modern technology, such as cloud computing, Internet of Everything, and big data analytics—all of which are predicated on the broader and more interconnected use of data.[1] Yet at the center of this digital highway lies a seemingly irresolvable

1. U.N. CONF. ON TRADE & DEV., DATA PROTECTION REGULATIONS AND INTERNATIONAL DATA FLOWS: IMPLICATIONS FOR TRADE AND DEVELOPMENT 108 (2016).

tension: open cross-border data flows versus restrictive data localization. Cross-border data flows can be thought of as the pillars of the digital highway as it refers to the movement or transfer of information across national borders.[2] Data localization, on the other hand, can be thought of as the tollbooths, as it refers to any measure that "specifically encumber(s) the transfer of data across national borders."[3] The more "tollbooths" are enacted, the more inefficient the highway becomes. This creates a kind of zero-sum game where greater data localization policies lead to more restrictive cross border data flows and vice versa.

To alleviate this tension, rules of the road must be established. Currently, there are few, if any, binding international or global treaties dealing with data privacy,[4] leaving many global technology and financial companies stranded in uncertain and uncharted territory.[5] The consequences for inaction on international data privacy framework are stark; not only are hundreds of billions of trade dollars at risk, but there is also an increased risk of a digital cold war.[6] Thus, the question is not *why* nations should reach international agreements on data privacy, but rather *how* such agreements can be made.

The zero-sum game between data localization and cross-border data flows creates a tragedy of the commons situation.[7] Given the tremendous importance of data in the modern era, both in terms of its economic value in the digital economy and its political value in national security affairs, countries are strongly incentivized to enact data localization policies to contain its data within its domestic borders. Yet, if every country enacts protectionist data localization policies, then the digital highway might collapse altogether. This balancing of competing incentives is further explored in Part III, which applies a game theory approach to understand whether it is possible to reach the pareto-optimal state of mutual cooperation.

---

2. Rachel F. Fefer, CONG. RSCH. SERV., R45584, DATA FLOWS, ONLINE PRIVACY, AND TRADE POLICY (2020).

3. Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, 19 WORLD TRADE REV. 341, 341 (2020).

4. Monika Zalnieriute, *An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance*, 23 INT'L J.L. & INFO. TECH. 99, 100 (2015).

5. *See, e.g.*, Tracy Qu, *Didi Cybersecurity Review Expected to Set Precedent for Future 'National Security' Probes into Data Collection*, S. CHINA MORNING POST (July 5, 2021, 5:00 PM), https://www.scmp.com/tech/big-tech/article/3139777/didi-cybersecurity-review-expected-set-precedent-future-national.

6. Marc Champion, *Digital Cold War*, BLOOMBERG (Dec. 12, 2019, 11:31 AM), https://www.bloomberg.com/quicktake/how-u-s-china-tech-rivalry-looks-like-a-digital-cold-war.

7. The Tragedy of the Commons refers to a classical game theory scenario, where the best outcome for all parties is to cooperate but each party has selfish incentives not to cooperate. In the scenario, imagine that there is an open pasture for all herders and each herder wants to maximize their number of cattle. However, if there are too many cattle, then the pasture would run dry, leading to the starvation of all cattle. *See* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1244 (1968).

Additionally, even if some countries share the incentive to create binding international data privacy agreements, there are numerous obstacles preventing the formation and execution of such agreements. Part I discusses the cultural, legal, and administrative concerns. From a cultural perspective, many countries have fundamentally different conceptions and values concerning data privacy and individual privacy.[8] For example, for countries that prioritize state surveillance over individual privacy, it can be enormously difficult to reach any kind of common understanding necessary for an agreement to take place. From a legal perspective, even after an agreement is reached, it may not be enforceable due to conflicting jurisdictional issues and complex dispute resolution procedures. Worse still, many existing data privacy agreements conflict with one another or suffer significant gaps in coverage, leading to legal ambiguity and uneven enforcement. From an administrative perspective, since enforcement can be costly and cumbersome, some countries may simply lack the resources or the incentives to adequately enforce the existing data privacy agreements.

Despite these obstacles, a few international data privacy agreements have been reached throughout Europe, Asia, and the Americas. In Part II, this Note examines how such agreements were reached, how these agreements are enforced, and how effective these agreements actually are in practice. To evaluate the effectiveness of such agreements, particular emphasis is placed on flexibility and administrability, as such agreements must be flexible enough to accommodate different legal regimes and efficient enough to justify the costs of enforcement.

Part III focuses on the Safe Harbor Agreement between the United States and the European Union as a case study on the core vulnerabilities of international data privacy agreements. The Note applies a game theory approach to highlight why the current incentive structures are insufficient to induce mutual cooperation. Part IV proposes potential solutions to overcome the current gridlocks and obstacles, such as attaching data privacy requirements to trade agreements, discretionary enforcement mechanisms, and unilateral extraterritorial approaches. Part V concludes.

I. OBSTACLES TO INTERNATIONAL DATA PRIVACY AGREEMENTS

Reaching an international agreement is never an easy feat. Given the enormous financial stakes, the political repercussions, and the sensitive nature of data privacy itself, data privacy agreements present numerous unique challenges. This Part addresses a few key challenges and elaborates why they can be so difficult to overcome. These challenges become a recurring theme

8. Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 139 (2017) (discussing how the European Union views data protection under a rights model where data protection is an inalienable human right whereas the United States follows a market model where data is a freely transferrable commodity).

throughout data privacy agreements across various global regions and are explored further in Parts II through IV.

A. *Digital Sovereignty & Cultural Values*

Data localization is often motivated by state sovereignty, which consists of three core elements: (1) supreme control, (2) over a territory, with (3) independence from other sovereigns.[9] To exercise digital state sovereignty, a state may use its "impressive arsenal of tools" to assert control over its internet, such as controlling network architecture, promoting state censorship and mandating compliance with internet regulations.[10] The extent to and manner in which a state exercises its digital sovereignty is closely aligned with its cultural values, as illustrated through the following examples of China, the United States, and the EU.

China follows a control model for its data privacy framework, where its data protection regime is more concerned with what information gets into the country than what information leaves it. To achieve this objective, China adopted a policy of "guarded openness" to harness the economic benefits of the digital revolution while protecting its position against foreign influence.[11] This approach is reflected through both its domestic and international data privacy policies. Domestically, Chinese regulators have replaced the Great Firewall with the Golden Shield. Whereas the Great Firewall was designed to restrict internet access, the Golden Shield is designed to monitor internet access, i.e., shifting the regulatory focus from generalized content control at the gateway level to individual surveillance of users at the edge of the network.[12] Internationally, Chinese policymakers recently passed the Personal Information Protection Law ("PIPL"), which carries far reaching extraterritorial application and focuses on data localization.[13] The PIPL requires state regulatory approval for cross-border data transfers (e.g., pass national security

9. Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 360 (2018).

10. *Id.* at 361.

11. Ryan Moshell, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 419 (2005); *see also* Ping Punyakumpol, *The Great Firewall of China: Background*, TORFOX (June 1, 2011), https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/author/pingp/index.html.

12. Moshell, *supra* note 11, at 419.

13. The PIPL applies to any entity that processes the data of any natural persons in Mainland China, even if that entity is not physically located within the territory of Mainland China or conduct any business within China. *See* Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), arts. 3, 53.

assessment, undergo personal information protection certification, etc.),[14] and enforces harsh consequences for non-compliance.[15]

The United States follows a market model for its data privacy framework, where personal information is just another commodity in the market, rather than a fundamental right. As such, the focus of informational privacy law in the United States is policing fairness in the exchanges of personal data.[16] This is exemplified through the Federal Trade Commission's (FTC) regulatory authority and the data broker industry. The FTC's regulatory authority is derived from Section 5(a) of the FTC Act, which allows the FTC to prohibit any "unfair or deceptive acts or practices."[17] As the text suggests, this policy's chief purpose is to police the fairness of the data exchange market rather than to prevent its existence.[18] With respect to data brokers, entities that collect and sell consumer information, the FTC recommended various proposals to enhance transparency, but it did little to clamp down on the brokers' aggressive data collection practices.[19] This illustrates that the FTC does not wish to restrict the data market altogether, but rather to ensure that the market is free, transparent, and fair.

Finally, the EU follows a rights model for its data privacy framework, where data protection is an unalienable "fundamental right."[20] This strong emphasis on data privacy protections has made the EU the de facto leader in crafting international data privacy agreements, as exemplified through the

14. *Id.* art. 38.

15. For violations of PIPL, Chinese authorities may issue an order for rectification, issue warmings, confiscate any unlawful income, suspend businesses, or impose a fine of up to 5% of annual turnover for the previous year. *Id.* art. 66.

16. *See* Schwartz & Peifer, *supra* note 8, at 132.

17. The FTC regulates consumer privacy issues, which include data security practices, through Section 5(a) of the Federal Trade Commission Act. 15 U.S.C. §45(a)(1) states: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."

18. In *Schrems v. Data Protection Commissioner*, the Court of Justice of the European Union (CJEU) found that the FTC's jurisdiction covers "unfair or deceptive acts and practices in commerce and therefore does not extend to the collection and use of personal information for non-commercial purposes. . . . The FTC was established not, as is the case within the European Union of the national supervisory authorities, to ensure the protection of the individual right of privacy, but to ensure fair and trustworthy commerce . . . ." Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:627, ¶ 205 (Sept. 23, 2015).

19. *See generally* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014). Notably, data brokers have very significant influence and market power. The FTC found that one data broker had 3,000 data segments for nearly every U.S. consumer, and another broker added three billion new records each month to its databases. *Id.* at 47–47. Data brokers sometimes place cookies on a consumer's browser without the consumer's knowledge, so that it may track the consumer's online and offline activities. *Id.* at 47. These online and offline activities are then aggregated to make sensitive inferences about the consumers, which are then packaged and sold to other entities. *Id.*

20. Schwartz & Peifer, *supra* note 8, at 123.

General Data Protection Regulation ("GDPR")[21] and the Council of Europe Convention.[22]

These differing attitudes towards data privacy can make it incredibly difficult to reach an agreement on universal data privacy regulations. In a speech to cybersecurity regulators, Chinese President Xi Jinping defined cyber sovereignty as "respecting each country's right to choose its own internet development path, its own internet management model, [and] its own public policies on the internet."[23] In another example, when the EU first adopted its data directive, EU officials had hoped to convince reluctant U.S. lawmakers to adopt a similar approach. However, this effort failed due to their "fundamentally differing conceptions of liberty."[24]

B. *Gaps in Legal Coverage*

Some countries do not have data privacy laws in place or lack sufficient understanding of the legal issues surrounding data privacy and protection. A study conducted by the United Nations Conference on Trade and Development ("UNCTAD") found that roughly thirty percent of countries have no data privacy laws in place, and more than sixty percent of government representatives in forty-eight countries in Africa, Asia, and Latin America reported difficulties in understanding legal issues related to data protection and privacy.[25] This lack of understanding is prevalent among the policymakers, the court adjudicators, and the national regulators, as seen with Figures 1 and 2 below.[26] To reach meaningful international data privacy agreements, it is imperative to address these gaps in legal coverage.

---

21. Regulation 2016/679, of the European Parliament and of the Council of 27 April 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 [hereinafter GDPR].

22. Regulation 2018/1725, of the European Parliament and of the Council of 23 October 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation 45/2001/EC, 2018 O.J. (L 295).

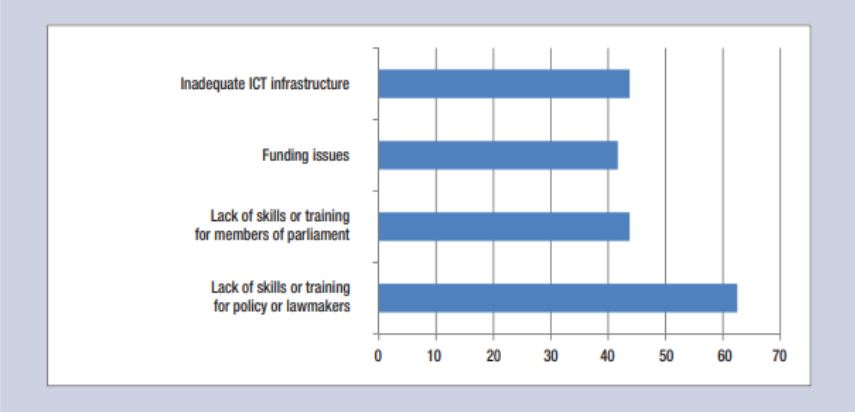
23. Franz-Stefan Gady, *The Wuzhen Summit and the Battle over Internet Governance*, THE DIPLOMAT (Jan. 14, 2016), https://thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-internet-governance.

24. Daniel R. Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement*, 41 CASE W. RSRV. J. INT'L L. 193, 199 (2009).

25. U.N. CONF. ON TRADE & DEV., *supra* note 1, at 8.

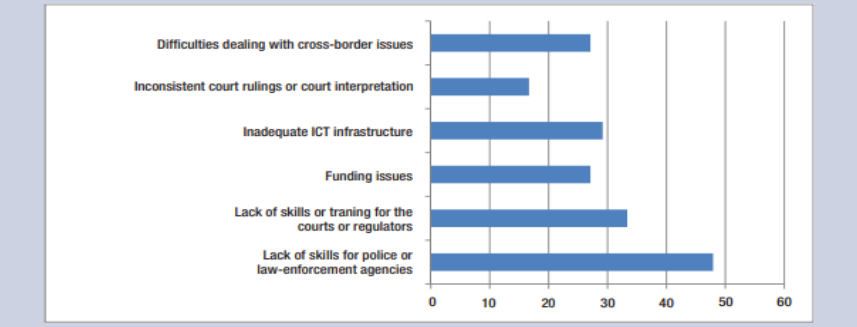
26. *Id.* at 8–9.

Figure 1. Challenges faced by ASEAN countries and selected countries in the ECOWAS, Latin America and the Caribbean (48 countries) in enacting data protection legislation.



Source: UNCTAD

Figure 2. Challenges faced by ASEAN countries and selected countries in the ECOWAS, Latin America and the Caribbean (48 countries) in enforcing data protection legislation.



Source: UNCTAD

C. *Complex Dispute Resolution Procedures*

Jurisdiction can be a complicated issue for international dispute resolutions, as multiple countries may claim to have jurisdiction over the matter. Without clear jurisdiction, it is difficult to ascertain who can actually enforce the existing data privacy legislations.

One such notable case is the *Belgian Commission for the Protection of Privacy v. Facebook Ireland Ltd.*,[27] where Belgian regulators discovered that Facebook had violated Belgian privacy laws by placing cookies and other hidden tracking tools through its social plug-ins to track the online activities

27. Case C-645/19, Facebook Ireland Ltd. v. Gegevensbeschermingsautoriteit, ECLI:EU:C:2021:483 (June 15, 2021).

of anyone, including non-Facebook users, who visited the site.[28] Belgian regulators argued that because some of the affected users were Belgian citizens and because Facebook had a subsidiary in Belgium whose lobbying and public administration activities were "inextricably linked" with its data processing activities, Belgian courts had the jurisdiction to prosecute the case.[29] The Belgian court agreed and fined Facebook 250,000 euros per day until Facebook complied with Belgian regulators.[30] However, Facebook appealed the decision to the Brussels Appeals Court, arguing that because Facebook has its European headquarters in Ireland, only the Irish Data Protection Commissioner ("DPC") has jurisdiction over how Facebook uses European's data. The Brussels Appeals Court agreed and dismissed the case, securing a major victory for Facebook.[31]

D. *Administrability Concerns*

While data privacy regulations are great in theory, they can also be prohibitively expensive for both companies to comply with and for regulators to enforce. For companies, more regulations often entail higher compliance costs. For example, Article 24 of the GDPR requires data controllers to implement "appropriate technical and organisational measures."[32] These measures include: implementing data mapping and records of processing activities, creating systems to record and manage ongoing consent, providing data protection awareness training for all employees, establishing a process to recognize and respond to individuals' requests to access their personal data, and more.[33] Given these significant compliance costs, many companies,

28. Julia Fioretti, *Facebook Wins Privacy Case Against Belgian Data Protection Authority*, REUTERS (June 29, 2016, 11:00 AM), https://www.reuters.com/article/us-facebook-belgium/facebook-wins-privacy-case-against-belgian-data-protection-authority-idUSKCN0ZF1VV. Facebook gets some data on non-users from people on its network, such as when a user uploads email addresses of friends. Other information comes from "cookies," small files stored via a browser and used by Facebook and others to track people on the internet, sometimes to target them with ads. David Ingram, *Facebook Fuels Broad Privacy Debate by Tracking Non-Users*, REUTERS (Apr. 15, 2018, 7:04 AM), https://www.reuters.com/article/us-facebook-privacy-tracking/facebook-fuels-broad-privacy-debate-by-tracking-non-users-idUSKBN1HM0DR.

29. Marcus Evans & Jay Modrall, *Belgian Court Orders Facebook to Stop Tracking Non-Members, Rejects FB's Assertion of Lack of Jurisdiction*, NORTON ROSE FULBRIGHT DATA PROT. REP. (Nov. 23, 2015), https://www.dataprotectionreport.com/2015/11/belgian-court-orders-facebook-to-stop-tracking-non-members-rejects-fbs-assertion-of-lack-of-jurisdiction.

30. Fioretti, *supra* note 28.

31. *Belgian Privacy Commission v. Facebook Ireland Limited*, COLUM. U. GLOB. FREEDOM OF EXPRESSION, https://globalfreedomofexpression.columbia.edu/cases/belgian-privacy-commission-v-facebook (last visited Apr. 15, 2022); *see also Facebook Ireland Ltd.*, ECLI:EU:C:2021:483.

32. GDPR, *supra* note 21, art. 24(1).

33. *GDPR Compliance Checklist for Controllers*, GDPR REG. (Sept. 8, 2020, 1:36 PM), https://www.gdprregister.eu/gdpr/gdpr-checklist-for-controllers.

particularly smaller digital advertising firms and media outlets, have opted to exit the EU market entirely to avoid any potential (and costly) violation.[34] Smaller companies are particularly concerned with regulatory enforcement since many believe that they are "easy hits" as they are unable to afford lawyers to defend themselves in case of violation.[35] By enacting higher barriers of entry through increased compliance costs, the GDPR prices out smaller companies and entrenches the dominance of BigTech.[36]

For regulators, they often lack the necessary budgets to adequately enforce their ballooning responsibilities under the GDPR. In a recent 2020 survey of privacy regulators in thirty European countries, twenty-one country representatives responded that they did not have sufficient resources to carry out their obligations under the GDPR.[37] Notably, the Irish DPC, the primary agency responsible for enforcing the GDPR, received an annual budget increase of only two million euros, roughly a third of what it had requested, bringing its total to just 16.9 million euros.[38] For comparison, Facebook Ireland's revenues average over 94 million euros per day, or 34.32 billion per year.[39] Given such a large discrepancy, it is unsurprising that Irish regulators are unable to enforce data privacy protections. In fact, the Irish DPC has delivered decisions in only two percent of EU-wide cases where it was the lead

34. Since the implementation of the GDPR in 2018, more than 1,000 companies, mainly U.S.-based newspapers, have exited the EU market to avoid dealing with the burdensome GDPR compliance requirements. *Websites Not Available in the European Union After GDPR*, VERIFIEDJOSEPH (Mar. 20, 2019, 7:53 PM), https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr; *see also* Hannah Kuchler, *US Small Businesses Drop EU Customers over New Data Rule*, FIN. TIMES (May 24, 2018), https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

35. In the 2019 GDPR Small Business survey, 86% of business leaders said it was essential to comply with the GDPR and cited the fear of grave penalties as a major motivating factor. GDPR.EU, 2019 GDPR SMALL BUSINESS SURVEY 5 (2019), https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf.

36. GDPR compliance cost the world's 500 largest corporations $7.8 billion. Mehreen Khan, *Companies Face High Cost to Meet New EU Data Protection Rules*, FIN. TIMES (Nov. 19, 2017), https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc; *see also* Ivana Kottasová, *These Companies are Getting Killed by GDPR*, CNN BUSINESS (May 11, 2018, 6:39 AM), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html (noting that "[t]he implications and ramifications of GDPR compliance will challenge numerous organizations . . . with resources on scales smaller than, say—and in particular—Facebook and Google").

37. Adam Satariano, *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, N.Y. TIMES (Apr. 28, 2020), https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html.

38. Derek Scally, *German Regulator Says Irish Data Protection Commission is Being 'Overwhelmed'*, IRISH TIMES (Feb. 3, 2020, 5:27 AM), https://www.irishtimes.com/business/financial-services/german-regulator-says-irish-data-protection-commission-is-being-overwhelmed-1.4159494.

39. Gordon Deegan, *Facebook Ireland Revenues Surge to €94m Per Day for 2019*, IRISH TIMES (Dec. 9, 2020, 6:48 AM), https://www.irishtimes.com/business/economy/facebook-ireland-revenues-surge-to-94m-per-day-for-2019-1.4431080.

authority.[40] Without the resources for enforcement, the GDPR requirements might be more bark than bite, especially for the BigTech companies that can afford the legal expenses and penalties in the rare event that they do occur.

II. EXISTING INTERNATIONAL AND REGIONAL DATA PRIVACY INITIATIVES

Despite the many obstacles, some countries initiated international data privacy initiatives as early as the 1960s.[41] However, progress has been gradual and piecemeal. To date, there is still no singular international data privacy agreement that binds all countries; instead, there are multiple overlapping, and at times conflicting, data privacy agreements between various geographical regions. Part II primarily looks to four key international agreements: (i) the General Data Protection Regulation ("GDPR"); (ii) the Personal Information Protection Law ("PIPL"); (iii) the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines"); and (iv) Asia-Pacific Economic Cooperation Cross-Border Privacy Rules ("APEC CBPRs"). Each of the following agreements are given a broad overview before diving into its various advantages and disadvantages.

A. *GDPR*

1. Overview

Drafted and passed by the European Parliament in 2016, the General Data Protection Regulation (GDPR) is arguably one of the toughest privacy and security regulations in the world.[42] The GDPR has an incredibly far-reaching extraterritorial effect. Any organization that collects, targets, monitors, or processes data related to people in the EU must comply with the GDPR

40. JOHNNY RYAN, IRISH COUNCIL FOR C.L., ECONOMIC & REPUTATIONAL RISK OF DPC'S FAILURE TO UPHOLD EU DATA RIGHTS 7 (2021), https://www.iccl.ie/digital-data/economic-reputational-risk-of-the-dpcs-failure-to-uphold-eu-data-rights; *see also* Jenny Darmody, *Facebook Dominates Irish Data Protection Investigations*, SILICON REPUBLIC (Feb. 25, 2021), https://www.siliconrepublic.com/enterprise/data-protection-commission-facebook (finding that out of 6,600 valid breach notifications in 2020, the Irish DPC was only able to engage in "six or seven" investigations).

41. For example, the Council of Europe started its work in the data privacy field as early as 1968. Paul De Hert & Vagelis Papakonstantinou, *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?*, 9 I/S: J.L. & Pol'y 271, 272 (2013).

42. *What is the GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr (last visited Apr. 15, 2022).

guidelines.[43] These guidelines codify core data protection principles,[44] expand individual privacy rights,[45] and impose additional obligations on companies to process, store, and transfer individual data outside of the European Economic Area ("EEA").[46] The penalties for violating the GDPR can be stark. Minor infringements can result in a fine of up to 10 million euros, or two percent of the firm's worldwide revenues (whichever amount is higher), and major infringements can double that penalty.[47]

For organizations to comply with the GDPR, they can implement Binding Corporate Rules ("BCR") or insert Standard Contractual Clauses ("SCC").[48] Under the BCR approach, organizations can draft their own data protection rules and submit them to the European Commission for approval.[49] If these rules incorporate the general data protection principles into the organization's privacy policy and provide a sufficient degree of protection for the transfer of personal data,[50] then the European Commission may consider these rules to be GDPR compliant.[51] One major advantage of BCRs is its flexibility, as companies may tailor the rules to best suit their operational needs. Additionally, by drafting its own privacy rules, companies may have more awareness of their own privacy procedures and of the GDPR requirements generally. This awareness could translate to greater overall compliance. On the other hand, this process can be labor intensive and time

43. GDPR, *supra* note 21, art. 3.

44. The GDPR sets out seven data protection principles: (i) lawfulness, fairness and transparency, (ii) purpose limitation, (iii) data minimization, (iv) accuracy, (v) storage limitation, (vi) integrity and confidentiality, and (vii) accountability. *Id.* art. 5.

45. The GDPR expanded EU citizens' privacy rights to include: (i) right to be informed, (ii) right to access, (iii) right to rectification, (iv) right to erasure, (v) right to restrict processing, (vi) right to data portability, (vii) right to object, and (viii) rights in relation to automated decision making and profiling. *Id.* arts. 12–22.

46. Organizations covered by the GDPR must follow additional obligations including: (i) the appointment of a Data Protection Officer, (ii) the implementation of appropriate data security measures, and (iii) the obtainment of affirmative consent from data subjects. *Id.* arts. 37, 44–49.

47. Ben Wolford, *What are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines (last visited Apr. 15, 2022). Minor infringements may include any violations of the articles governing the following: controllers and processors (arts. 8, 11, 25–39, 42, 43); certification bodies (arts. 42–43); and monitoring bodies (art. 41). *Id.* Major infringements, on the other hand, go against the very principles of the right to privacy and the right to be forgotten. These include any violations of the articles governing the following: the basic principles of data processing (arts. 5, 6, 9); the conditions for consent (art. 7); the data subjects' rights (arts. 12–22); the transfer of data to an international organization or a recipient in a third country (arts. 44-49); any violation of member state laws adopted under Chapter IX; and non-compliance with an order by a supervisory authority. *Id.*

48. GDPR, *supra* note 21, art. 46(2).

49. *Id.* art. 47.

50. *Id.* art. 47(2).

51. *See* U.N. CONF. ON TRADE & DEV., *supra* note 1, at 33.

consuming. For most companies, receiving approval for BCRs takes about eighteen months,[52] and any updates to the BCR may require new authorization.[53]

Under the SCC approach, the European Commission drafted model contractual clauses that organizations can directly insert into their privacy policies to be GDPR compliant.[54] Each European member state's supervisory authority can also adopt their own SCCs to be inserted for their region.[55] However, since the previous SCCs were developed in 2001 and predated the GDPR, many of its provisions were outdated and did not sufficiently adapt to the evolving data privacy needs brought on by new technology.[56] In response, on June 4th, 2021, the European Commission issued two new sets of SCCs

52. Angelique Carson, *How Did Corning Get BCRs in Just Six Months? Well, They'll Tell You*, IAPP (Jan. 7, 2016), https://iapp.org/news/a/how-did-corning-get-bcrs-in-just-six-months-well-theyll-tell-you.

53. To receive approval, the company must first determine the following: (1) relevant group companies, (2) EEA members with data protection responsibilities, and (3) BCR lead. After these determinations, the company may draft the BCRs and submit its proposal to the DPO for approval. If approved, the company must then distribute the BCRs to all relevant group companies and submit the BCR to both the company's board and the BCR lead for final authorization. This final review and authorization process lasts a minimum of twelve months, before the BCRs may be deemed effective. PRICEWATERHOUSECOOPERS, BINDING CORPORATE RULES: THE GENERAL DATA PROTECTION REGULATION 5, 15 (2019), https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf.

54. GDPR, *supra* note 21, art. 28(7); *see also Standard Contractual Clauses for International Transfers*, EURO. COMM'N (June 4, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

55. GDPR, *supra* note 21, art. 57(1)(j).

56. The old SCCs were relatively inflexible and were only structured to cover data transfers between countries inside the EU and countries outside of the EU. The new SCCs is structured to contain "modules" that can be swapped in and out depending on whether the transfer is from a "controller" (i.e., those who determine the purposes for which the data will be processed) to a "processor" (i.e., those who processes the data on behalf of the controller), controller to controller, processor to processor, or processor to controller. *See* Jörg Hladjk et al., *New Standard Contractual Clauses by the European Commission: What You Need to Know*, JONES DAY (June 2021), https://www.jonesday.com/en/insights/2021/06/new-standard-contractual-clauses-by-the-european-commission-what-you-need-to-know; *see also New Standard Contractual Clauses Introduced for GDPR – Effective September 27, 2021*, HINCKLEY ALLEN (Sept. 27, 2021), https://www.hinckleyallen.com/publications/new-standard-contractual-clauses-introduced-for-gdpr-effective-september-27-2021.

The influential court case, Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd., ECLI:EU:C:2020:559 (July 16, 2020) ("Schrems II"), challenged the validity of the old SCCs and the Privacy Shield agreement between the United States and the EU. While Schrems II upheld certain aspects of the old SCCs, it also held that just inserting the SCCs alone may not be sufficient to fully comply with the GDPR. *See* Hunton Andrews Kurth's Priv. & Cybersecurity, *BREAKING: Unexpected Outcome of Schrems II Case: CJEU Invalidates EU-U.S. Privacy Shield Framework but Standard Contractual Clauses Remain Valid*, NAT'L L. REV. (July 16, 2020), https://www.natlawreview.com/article/breaking-unexpected-outcome-schrems-ii-case-cjeu-invalidates-eu-us-privacy-shield.

("New SCCs") to replace the old SCCs and address these concerns.[57] The first set of New SCCs mandates specific, compulsory clauses to be included in contracts between data controllers and processers.[58] To maintain their validity, these SCC clauses cannot be modified so as to detract or lessen its impact.[59] The second set of New SCCs requires the receiving country/countries to have "essentially equivalent" data privacy protections as the EU member states before any transfer of personal data to countries outside of the EU can occur.[60] To meet this requirement, organizations must create "transfer impact assessments" to assess whether the laws of the country into which the data is imported is consistent with the SCCs and the GDPR, and whether any "supplementary measures" are necessary to bolster data protections.[61] Despite these additional compliance requirements, the SCCs remain the preferred option to govern data transfers outside of the EU, as other transfer options are generally more burdensome or costly.[62]

For countries to comply with the GDPR, they must pass the adequacy determination (also known as the whitelist approach).[63] To meet this determination, a country must demonstrate to the European Commission that it offers an adequate level of data protection (i.e., on par with those in the EU).[64] The whitelist is vital when conducting a preliminary assessment as to whether a proposed processing is of high risk.

2. Advantages and Disadvantages

The GDPR is incredibly expansive, both to its benefit and to its detriment. For example, since the penalties are scalable,[65] the GDPR can, in theory, offer flexible and substantive deterrence. However, since some compliance costs are fixed, these costs may be much greater for small to medium enterprises ("SMEs") than for large enterprises. Take, for example, Article 37 of the GDPR which requires any enterprise whose core activities consist of processing data on a large scale to appoint a Data Protection Officer

57. Mallory Petroli, *New Standard Contractual Clauses Under the GDPR*, NAT'L L. REV. (Aug. 9, 2021), https://www.natlawreview.com/article/new-standard-contractual-clauses-under-gdpr.

58. *Id.*

59. *Id.*

60. *Id.*

61. Ryan P. Blaney et al., *Navigating the New Standard Contractual Clauses for International Data Transfer Under the GDPR*, NAT'L L. REV. (June 7, 2021), https://www.natlawreview.com/article/navigating-new-standard-contractual-clauses-international-data-transfers-under-gdpr.

62. *See* Ahmed Baladi et al., *European Commission Adopts New Standard Contractual Clauses for International Data Transfers and Data Processing Agreements*, GIBSON DUNN (June 14, 2021), https://www.gibsondunn.com/european-commission-adopts-new-standard-contractual-clauses-for-international-data-transfers-and-data-processing-agreements.

63. GDPR, *supra* note 21, art. 45.

64. *Id.* art. 45(2).

65. *Id.* art. 83.

(DPO).[66] This requirement is not dependent on the size of the company, but rather solely on the type of processing activities undertaken by the enterprise. Unfortunately, the types of processing activities in question are not clear because the GDPR does not define "core activities" or "large scale." If an enterprise fails to take precautionary measures or intentionally violates the GDPR, then the penalties can be magnified.[67] Given the vagueness of the criteria and the severe repercussions for negligence, many SMEs are confronted with a difficult and costly choice—either appoint a fully-salaried DPO or exit the EU market altogether. It is thus unsurprising that hundreds of small digital advertising companies have pushed to leave the EU due to the GDPR, thereby concentrating the $200 billion global digital advertising within the hands of a few BigTech giants such as Facebook and Google.[68]

Furthermore, given its breadth, regulators often have too many cases and too few resources. The European Center for Digital Rights found that despite reporting more than 10,000 complaints in 2020, the Irish DPC only issued six to seven decisions, meaning that only 0.07% of all GDPR complaints might see a formal decision.[69] This lack of enforcement tarnishes both the reputation of regulators as well as that of the GDPR itself, as organizations may see its regulations as nothing more than empty threats. In fact, since the GDPR was enacted in 2018, Google has been the only giant tech company to be penalized—a fine of 50 million euros.[70]

Additionally, with greater territorial scope comes greater jurisdictional issues. Under Article 79(2), the GDPR allows any EU citizen to bring their private enforcement action in the member state where the controller or processor has an establishment, or alternatively, in the member state where the data subject has their habitual residence.[71] Since the CJEU interpreted the term "establishment" very broadly,[72] plaintiffs can file complaints in

66. The DPO must have "expert knowledge of data protection law." *Id.* art. 37. It must also not have any conflicts of interest (e.g., the enterprise's legal counsel and head of IT both may not serve as DPO). Julia Kaufmann & Jan-Philipp Guenther, *Data Protection Officers Must Not Have a Conflict of Interest – Part 2*, GLOBAL COMPLIANCE NEWS (Jan. 9, 2018), https://www.globalcompliancenews.com/2018/01/09/data-protection-officers-conflict-interest-20180109.

67. To calculate a GDPR fine, regulators consider the following ten factors: (1) gravity and nature, (2) intention, (3) mitigation, (4) precautionary measures, (5) history, (6) cooperation, (7) data category, (8) notification, (9) certification, and (10) aggravating and mitigating factors. Wolford, *supra* note 47.

68. Kate Holton, *Europe's New Data Law Upends Global Online Advertising*, REUTERS (Aug. 23, 2018, 2:07 AM), https://www.reuters.com/article/us-advertising-gdpr-insight/europes-new-data-law-upends-global-online-advertising-idUSKCN1L80HW.

69. *Irish DPC "Handles" 99,93% of GDPR Complaints, Without Decision?*, NOYB (Apr. 28, 2021), https://noyb.eu/en/irish-dpc-handles-9993-gdpr-complaints-without-decision.

70. Satariano, *supra* note 37.

71. GDPR, *supra* note 21, art. 79(2).

72. *See* Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639, ¶ 31 ("[T]he concept of 'establishment', within the

establishments where they have minimal connection, leading to extensive forum shopping.[73]

Thirdly, both the SCC and the BCR approach can be overly bureaucratic and costly. For the SCC approach, simply inserting the new SCCs are not sufficient to comply with the GDPR.[74] Instead, organizations may likely need to implement additional, ongoing safeguards (e.g., user encryption, internal IT security management, periodical certification, etc.).[75] Such safeguards incur greater compliance costs and may price out SMEs from the EU market. Similarly, the complex and cumbersome BCR approval process has led some scholars to describe the BCR as "data protection for the rich."[76] As such, the GDPR may entrench the concentration of BigTech, hurting consumers and businesses alike.

Finally, while the adequacy determination allows entire jurisdictions to transfer data, thereby circumventing the issues of piecemeal determinations associated with the BCR and SCC approaches, adequacy determinations suffer from serious defects. These include inconsistent applications, jurisdictional uncertainties, and lack of appreciation for legal pluralism.[77] For example, the United States was unable to receive an adequacy determination because of the differing conceptions between the United States and the EU for what the "right to data protection" actually means.[78] Thus, the question as to what general data protection in the United States is adequate according to EU standards is left largely unanswered. As a result, most countries are unable to rely on adequacy determinations to transfer data flows to the EU.[79]

---

meaning of Directive 95/46, extends to any real and effective activity—even a minimal one—exercised through stable arrangements.").

73. *See* Ioannis Revolidis, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, 11 MASARYK U. J.L. & TECH. 7, 27 (2017).

74. *See* Tess Blair & Axel Spies, *New European Standard Contractual Clauses are Not 'Set and Forget'*, MORGAN LEWIS (June 14, 2021), https://www.morganlewis.com/pubs/2021/06/new-european-standard-contractual-clauses-are-not-set-and-forget.

75. *See* EUR. DATA PROT. BD., RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA (2020), https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

76. Sylwia Pietrzak, Transborder Data Flows: Binding Corporate Rules as a Global Transfer Mechanism and Trusted Data Processing Area (Jan. 2017) (Master Thesis, Tilburg University), http://arno.uvt.nl/show.cgi?fid=142708.

77. *See generally* Jennifer Stoddart et al., *The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research*, 44 J.L. MED. & ETHICS 143, 144 (2016).

78. Vagelis Papakonstantinou & Paul De Hert, *PNR Agreement and Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic*, 46 COMMON MKT. L. REV. 885, 898 (2009).

79. To date, only twelve countries have met the adequacy determination: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. *Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection*, EURO. COMM'N, https://ec.europa.eu/info/law/law-

B. *PIPL*

1. Overview

The Personal Information Protection Law ("PIPL"), adopted on August 20, 2021, by the Standing Committee (the top leadership of the Chinese Communist Party), provides the core regulatory framework for China's approach towards protecting data privacy.[80] The PIPL is, in many ways, China's answer to the GDPR as many of its provisions mirror those of the GDPR. Similar to the GDPR, the PIPL carries far-reaching extraterritorial effect. Under Article 3, the PIPL covers any entity that handles "personal information activities for the purpose of offering products or services to natural persons in Mainland China, or analyzing and assessing the behaviors . . . [of such] persons."[81] Next, the PIPL reiterates many of the same data protection principles and individual data privacy rights as the GDPR.[82] Third, the penalties for noncompliance are even more severe than those under the GDPR, with minor violations resulting in fines up to 1,000,000 RMB (roughly $158,000 USD), and major violations resulting in fines up to five percent of annual turnover for the previous year.[83] Unfortunately, the PIPL fails to define what constitutes "minor" and "major" violations, and there has not been any PIPL enforcement actions yet to further clarify the matter.

To comply with the PIPL, companies must adopt strict data localization procedures,[84] undergo regular compliance audits,[85] hire local governance staff,[86] and establish independent bodies to supervise personal information protection circumstances.[87] Most crucially, the PIPL enacts multilevel barriers for cross-border data transfers, including the approval from the Cybersecurity Administration of China ("CAC").[88] To receive CAC approval, the

topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Apr. 15, 2022).

80. Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) (China).

81. *Id.* art. 3.

82. *See, e.g.*, *id.* arts. 44–47 (establishing the right to restrict or refuse processing of data, right to data portability, right to correction, and right to erasure, respectively); *see also id.* arts. 3, 6 (establishing the principles of openness and transparency when handling personal information and the principle of data minimization respectively).

83. *Id.* art. 66.

84. *See id.* art. 40 (requiring entities that process a large volume of personal information to locally store personal information collected in China).

85. *Id.* art. 54.

86. *Id.* art. 53.

87. *Id.* art. 58.

88. To transfer data abroad, firms must obtain individual consent from the affected parties, register the transfer with the government, implement technical security measures to prevent foreign-government access to the data, and track onward transfers to other entities. *See* Jay Cline et al., *10 Ways China's New Data Rules Will Change Your Business*, PwC (Nov. 22, 2021),

firm can either pass the CAC security assessment, receive prior CAC certification, or enter into a standard form transfer agreement drafted by the CAC.[89] The CAC certification closely resembles the approved "certification mechanisms" in the GDPR,[90] while the standard form transfer agreement closely mirrors the GDPR's SCC approach. However, unlike the GDPR, the PIPL does not mention an adequacy determination for cross-border data transfers, suggesting that such transfers may be subject to greater regulatory scrutiny under the PIPL than under the GDPR.[91]

2. Advantages and Disadvantages

The PIPL's parallels with GDPR are unlikely to be purely coincidental. The inclusion of the same core data privacy principles and the individual data rights as the GDPR in the PIPL is particularly significant since it demonstrates Chinese policymakers' efforts to harmonize the two data privacy frameworks, despite not sharing the same cultural or political values towards data privacy.[92] This may reflect the beginning stages of developing international customs and norms surrounding data privacy. From this, it is possible that these data privacy principles could be absorbed into the "general principles of law recognized by civilized nations,"[93] and may serve as a common ground for future negotiations.

However, like the GDPR, the PIPL creates cumbersome compliance obligations. In fact, major technology firms such as Yahoo!, LinkedIn, and Epic Games have all recently announced their departure from China in light of the PIPL compliance challenges.[94] This vacuum could leave China's internet increasingly isolated and the global network increasingly fragmented. Additionally, the PIPL is noticeably vague in several key respects. For example, neither the PIPL nor the CAC has determined the threshold for "significant amounts of personal data." This threshold is particularly important for SMEs, since those that meet the threshold must hire data protection officers and

---

https://www.pwc.com/us/en/tech-effect/cybersecurity/china-pipl-rules-impact.html; *see also* Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), art. 38 (China).

89. Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), arts. 38, 40 (China).

90. *See* GDPR, *supra* note 21, art. 42(2).

91. *See* Jet (Zhisong) Deng & Ken (Jianmin) Dai, *The Comparison Between China's PIPL and EU's GDPR: Practitioners' Perspective*, DENTONS (Oct. 8, 2021), https://www.dentons.com/en/insights/articles/2021/october/8/the-comparison-between-chinas-pipl-and-eus-gdpr.

92. *See* Part I.A.

93. Statute of the International Court of Justice art. 38, June 26, 1945, 33 U.N.T.S 993.

94. Zen Soo, *EXPLAINER: Why Are Foreign Tech Firms Pulling Out of China*, AP NEWS (Nov. 3, 2021), https://apnews.com/article/technology-business-china-hong-kong-data-privacy-2f320c0af956d3794fb7c9957fa33487.

adhere to stricter data localization requirements.[95] Absent this clarification, SMEs may err on the side of caution and exit the Chinese market altogether. With less competition, dominant industry players could consolidate their market position, increase the costs of their services, and hurt consumers overall.

Finally, whereas the GDPR was ratified by a coalition of countries, the PIPL is ratified solely by China. The PIPL's unilateral approach towards extraterritorial enforcement may be viewed by other countries as undermining their national sovereignty, which in turn, diminishes international comity. Derived from territorial sovereignty, international comity refers to the "discretionary doctrine that empower[s] courts to decide when to defer to foreign law out of respect for foreign sovereigns."[96] By supporting comity, the "interests of both forums are advanced—the foreign court because its laws and policies have been vindicated; the domestic country because international cooperation and ties have been strengthened. The rule of law is also encouraged, which benefits all nations."[97] However, extraterritoriality reflects a lack of respect to the views and interests of foreign sovereigns[98] and undercuts the "mutuality and reciprocity" that is fundamental for international comity.[99] Not only does this make future cooperation less likely, but it may also lead to complex jurisdictional disputes where multiple sovereigns have overlapping jurisdiction over the same dispute/violation. Suppose, for example, that Apple transferred its global sales data to a third-party financial auditor but had failed to verify whether the recipient also maintained adequate data protection procedures. Since the global sales data includes consumer information from both European and Chinese citizens, this transfer may be subject to both the GDPR and the PIPL compliance obligations. From here, at least two outcomes are possible. First, the respective enforcement authorities under the GDPR and PIPL could each individually pursue enforcement action, thus subjecting Apple to two (potentially major) penalties for the same violation. Second, one court may issue an anti-suit injunction (ASI) to prevent another party from continuing proceedings in another jurisdiction, which in turn, may

95. *See* Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), art. 52 (China) (requiring "personal information handlers that handle personal information *reaching quantities provided by the State cybersecurity and informatization department* [to] appoint personal information protection officers") (emphasis added); *see also id.* art. 40 (requiring "personal information handlers handling personal information *reaching quantities provided by State cybersecurity and informatization department* [to] store personal information collected and produced within the borders of the People's Republic of China domestically") (emphasis added).

96. Joel R. Paul, *The Transformation of International Comity*, 71 L. & CONTEMP. PROBS. 19, 20 (2008).

97. Laker Airways Ltd. v. Sabena, Belgian World Airlines, 731 F.2d 909, 937 (D.C. Cir. 1984).

98. *See* John DeQ Briggs & Daniel S. Bitton, *Heisenberg's Uncertainty Principle, Extraterritoriality and Comity*, 16 SEDONA CONF. J. 327, 328 (2015).

99. *See* Hilton v. Guyot, 159 U.S. 113, 164 (1895).

trigger the other jurisdiction to respond with an anti-anti-suit (AASI) injunction.[100] This could further jurisdictional uncertainty, increase transaction costs, and undermine international comity.

C. *OECD Guidelines*

1. Overview

In 1980, The OECD became the first international organization to have dealt expressly with the data privacy issue through its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines").[101] These Guidelines apply to OECD member states. The OECD currently consists of thirty-eight countries, [102] though it also encourages non-member states to join.

The OECD Guidelines' key contribution to the development of data privacy principles is its announcement of eight core data privacy principles: (i) collection limitation; (ii) data quality; (iii) purpose specification; (iv) use limitation; (v) security safeguards; (vi) openness; (vii) individual participation; and (viii) accountability.[103] Unfortunately, the OECD Guidelines are sparse with details regarding how such principles should be drafted or implemented and leaves the discretion entirely to member states.[104] Notably, the OECD Guidelines are non-binding. There are no fines or penalties associated with failing to abide by the guidelines, and no regulatory entity with enforcement authority.

---

100. An ASI permits a court to enjoin a litigant from commencing or continuing litigation in a foreign forum. ASIs are generally issued to protect a court's own legitimate jurisdiction or to prevent litigants' evasion of the forum's important public policies. However, since ASIs severely undermine international comity, courts are generally reluctant to issue them. *See* Taryn M. Fry, *Injunction Junction, What's Your Function? Resolving the Split over Antisuit Injunction Deference in Favor of International Comity*, 58 Cath. U. L. Rev. 1071, 1077–84 (2009).

Many countries have issued AASIs in recent years, including India and China, particularly in international IP disputes. *See* Guodong Du & Meng Yu, *How Chinese Courts Deal with Anti-Suit Injunctions in International IP Disputes*, CHINESE JUST. OBSERVER (July 25, 2021), https://www.chinajusticeobserver.com/a/how-chinese-courts-deal-with-anti-suit-injunctions-in-international-ip-disputes.

101. Hans Peter Gassmann, former Head of the OECD ICCP Division, 30 Years After: The Impact of the OECD Privacy Guidelines, Address at the OECD Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP) (Mar. 10, 2010).

102. *Our Global Reach*, OCED, https://www.oecd.org/about/members-and-partners (last visited Apr. 15, 2022).

103. Cécile de Terwangne, *Is a Global Data Protection Regulatory Model Possible?*, *in* REINVENTING DATA PROTECTION? 175, 182 (Serge Gutwirth et al. eds., 2009).

104. ORG. FOR ECON. COOP. & DEV. (OECD), GUIDELINES ON THE PROTECTION AND TRANSBORDER FLOWS OF PERSONAL DATA 17 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

2. Advantages and Disadvantages

The OECD Guidelines' intentional vagueness and non-binding nature are its greatest strength and its greatest shortcoming. Since the OECD Guidelines are non-binding, there has been a wide acceptance of its core principles across both member and non-member states.[105] This wide acceptance alleviates two major hurdles to reaching international data privacy agreements. First, by having wide acceptance of its principles, the OECD Guidelines present a shared foundation for countries to work together on. This mitigates some of the digital sovereignty and cultural value conflicts between different countries described in Part I.

Second, the OECD Guidelines help educate countries on the importance of data privacy and introduces the elements necessary for a good data privacy regime. This education is particularly useful for regulators in countries with poor data privacy regimes, since they may now have the requisite knowledge to pass better data privacy governance regimes and mitigate the gaps in legal coverage. However, since the principles are intentionally vague, they are more aspirational than practical. Since OECD Guidelines are non-binding, countries are not obligated to abide by any of its principles.

Finally, since OECD Guidelines give countries the discretion to craft their own privacy regimes, countries have enormous flexibility to tailor the laws based on their own circumstances. This flexibility encourages greater legal and cultural diversity and promotes legal pluralism. However, the lack of consistency could lead to fragmented approaches towards data privacy. Companies could exploit this regulatory arbitrage and engage in forum shopping, thereby potentially creating a "race to the bottom" for data privacy protections. Unfortunately, even though the OECD Guidelines acknowledge this reality, stating that conflicts of law issues are "bound to arise," it offers no guidance on how to resolve such conflicts and simply punts the issue to member states to figure out amongst themselves. [106] Without clear guidance on proper jurisdiction, it becomes exceedingly difficult for the OECD Guidelines to be adequately enforced.

D. *APEC CBPR*

1. Overview

Initiated in 2005 and implemented in 2015, the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules ("APEC CBPR") is the dominant international data privacy agreement in Asia. APEC CBPR includes twenty-

105. U.N. CONF. ON TRADE & DEV., *supra* note 1, at 26.
106. OECD, *supra* note 104, at 63.

one member states, all of whom commit to enforcing the CBPR system within their respective territory.[107] Some key initiatives of the APEC CBPRs are:

1) Development of common APEC Privacy Principles: (i) preventing harm; (ii) notice; (iii) collection limitation; (iv) uses of personal information; (v) choice; (vi) integrity of personal information; (vii) security safeguards; (viii) access and correction; and (ix) accountability.[108]

2) Implementation of a voluntary CBPR enforcement system consisting of four separate elements: (i) self-assessment; (ii) compliance review; (iii) recognition/acceptance; and (iv) dispute resolution and enforcement.[109]

3) Establishment of a success metric for the CBPR system based on the following criteria: (i) the effective protection of consumer personal information privacy; (ii) the flexibility of the implementation system while still providing certainty for system participants; and (iii) the minimization of the regulatory burden on businesses.[110]

2. Advantages and Disadvantages

The APEC CBPR enjoys broad membership thanks to its enormous flexibility[111] Like the OECD guidelines, the APEC CBPR uses non-binding and non-committal language for its core principles, so it is able to garner widespread support. Such support is essential in bringing about shared mutual

107. *What is the Cross-Border Privacy Rules System*, ASIA-PAC. ECON. COOP., https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system (last updated Oct. 2021). The twenty-one member states include: Russia, People's Republic of China, Vietnam, Thailand, Malaysia, Singapore, Republic of Korea, Japan, Chinese Taipei, Hong Kong (China), The Philippines, Brunei Darussalam, Papua New Guinea, Indonesia, Australia, New Zealand, Canada, the United States of America, Mexico, Peru, and Chile. *About APEC*, ASIA-PAC. ECON. COOP., https://www.apec.org/about-us/about-apec (last updated Sept. 2021).

108. ASIA-PAC. ECON. COOP., APEC PRIVACY FRAMEWORK 11–29 (2005) [hereinafter APEC CBPR], https://www.apec.org/docs/default-source/publications/2005/12/apec-privacy-framework/05_ecsg_privacyframewk.pdf?sfvrsn=d3de361d_1.

109. ASIA-PAC. ECON. COOP., APEC CROSS-BORDER PRIVACY RULES SYSTEM: POLICIES, RULES AND GUIDELINES 4 (2014), http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_desarrollos_APEC_3.pdf.

110. *Id.* at 14.

111. *See, e.g.*, APEC CBPR, *supra* note 108, at 7 ("In view of the differences in social, cultural, economic and legal backgrounds of each member economy, there should be flexibility in implementing these Principles."); *see also id.* at 31 ("[T]he Framework is meant to be implemented in a flexible manner than can accommodate various methods of implementation . . . as Member Economies deem appropriate.").

understandings, which alleviate digital sovereignty concerns, and reduce gaps in legal coverage for data privacy laws. However, given its non-binding nature, these principles might be more aspirational than practical, calling its enforceability into question.

Enforceability concerns are worsened by the APEC CBPR's voluntary participation system. Notably, the APEC CBPR gives significant deference to member states in paragraph 13, which states that the CBPR Framework is "not intended to impede governmental activities authorized by law when taken to protect national security, public safety, national sovereignty or other public policy."[112] This deference allows member states to escape from the APEC CBPR principles and obligations altogether. As a result, countries might simply pay lip service to these principles rather than to fully commit to them.

Finally, while the APEC CBPR's flexibility allows for greater legal pluralism, this also results in materially different privacy regimes between the APEC member states. Worse still, the APEC CBPR does not designate any specific regulatory authority or any specific jurisdiction to enforce its policies. As a result, jurisdictional issues will inevitably arise, leading to forum shopping, conflicting laws, and inconsistent applications of the APEC CBPR principles.

III. ISSUES WITH INTERNATIONAL DATA PRIVACY FRAMEWORKS: A CASE STUDY (SAFE HARBOR AGREEMENT BETWEEN THE UNITED STATES AND THE EU)

This Part looks to the Safe Harbor Agreement between the United States and the EU as an illustration of the various obstacles that impede international data privacy agreements. It also applies a game theory model to see how closely the theoretical outcome maps onto the actual formation and breakdown of the Safe Harbor Agreement.

A. *Safe Harbor—An Overview*

When the EU enacted the 1995 General Data Protection Directive ("1995 Directive"), it signaled a significant transatlantic legal and policy divergence. Under the 1995 Directive, the recipient country must have an "adequate" level of data protection (i.e., adequacy determination) before it could process EU citizens' data.[113] However, the United States failed to meet this adequacy determination, in part because it viewed data privacy as a side matter to its e-

112. *Id.* at 8.

113. Bilyana Petkova, *Domesticating the "Foreign" in Making Transatlantic Data Privacy Law*, 15 INT'L J. CONST. L. 1135, 1140–41 (2017).

commerce strategy.[114] In response, the United States and the EU signed the Safe Harbor Agreement in 2000, which allowed the transfer of personal data between EU member countries and the United States and finally reunited the two economies.[115] Interestingly, the Safe Harbor Agreement ended up being neither an international treaty nor a bilateral agreement, but rather two unilateral acts.[116] Under this Agreement, the United States adopted a condensed version of the 1995 Directive's fair information principles,[117] which the European Commission then approved for U.S. companies that would voluntarily self-certify with the U.S. Department of Commerce to comply with the Safe Harbor framework.[118] The Safe Harbor Agreement applied to any U.S. organization subject to the FTC, and the FTC was designated as the primary regulator in charge of enforcing the agreement.[119] However, the Safe Harbor Agreement was eventually invalidated in 2015 by the highly influential case, *Schrems v. Data Protection Commissioner* ("*Schrems I*"),[120] and subsequently replaced by the Privacy Shield Agreement in 2016.[121]

Despite its benefits, reaching the Safe Harbor Agreement was quite surprising as the EU and the United States had vastly different data privacy regimes, and the United States lacked an omnibus privacy law. As mentioned in Part I, the EU considers the protection of personal data as a fundamental

---

114. David Bach & Abraham L. Newman, *The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence*, 14 J. EUR. PUB. POL'Y 827, 833–835 (2007).

115. Martin A. Weiss & Kristin Archick, CONG. RSCH. SERV., R44257, U.S.–EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD (2016).

116. Petkova, *supra* note 113, at 1141.

117. These included seven fair information principles: (i) notice; (ii) choice; (iii) onward transfer; (iv) security; (v) consistency; (vi) access; and (vii) enforcement. Jeffrey B. Ritter et al., *Emerging Trends in International Privacy Law*, 15 EMORY INT'L L. REV. 87, 114–17 (2001).

118. Petkova, *supra* note 113, at 1141. To self-certify, companies must adhere to the seven Safe Harbor Privacy Principles. *Id.*

119. Weiss & Archick, *supra* note 115, at 6.

120. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:627, ¶ 205 (Sept. 23, 2015).

121. The Safe Harbor Agreement was invalidated because the "CJEU found that the Safe Harbor program did not adequately protect personal data from 'interference' from the US government 'founded on national security and public interest requirements.'" Courtney M. Bowman, *US-EU Safe Harbor Invalidated: What Now?*, PROSKAUER (Oct. 6, 2015), https://privacylaw.proskauer.com/2015/10/articles/european-union/us-eu-safe-harbor-invalidated-what-now.

The Privacy Shield was subsequently invalidated in *Schrems II* on similar grounds. Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020). Here, the CJEU found that the Privacy Shield still offered insufficient safeguards against U.S. authorities to collect personal data about EU data subjects, who lacked effective means to seek redress against the U.S. government. Tony DeBos et al., *What to Do Now That the EU-US Privacy Shield Framework Is Invalid*, ERNST & YOUNG (Sept. 28, 2020), https://www.ey.com/en_us/consulting/what-to-do-now-that-the-eu-us-privacy-shield-framework-is-invalid.

human right.[122] As such, data protection is incorporated into Articles 7 and 8 of the 2000 Charter of Fundamental Rights of the European Union and made binding on all EU members through the 2007 Treaty of Lisbon.[123] In contrast, the United States views data as a tradeable commodity, and does not place particular emphasis on privacy protections.[124] In fact, the United States does not have a comprehensive federal data privacy legislation. Instead, the United States has a patchwork privacy regime derived from multiple sources, including the U.S. Constitution,[125] state legislation,[126] and tort law.[127]

The United States also does not have a designated federal authority to enforce data privacy protections. While the FTC may issue regulations to combat certain "unfair" data security practices, there is still relatively little case law demonstrating the FTC's enforcement authority.[128] In its *Schrems I* decision, the CJEU was particularly concerned about the United States' ability to adequately enforce the Safe Harbor Agreement because the FTC lacked the "power to monitor possible breaches of principles for the protection of

122. *See* Part I.A.

123. Weiss & Archick, *supra* note 115, at 2.

124. *See* Part I.A.

125. While the U.S. Constitution did not expressly mention privacy rights, the Supreme Court has interpreted certain amendments, such as the First Amendment and the Fourth Amendment, to confer certain privacy rights. *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995) (holding that the First Amendment free speech protections also guaranteed the right to speak anonymously and to preserve the confidentiality of one's associations); *see also* Katz v. United States, 389 U.S. 347, 350 (1967) (holding that the Fourth Amendment's prohibition on unreasonable search and seizure extends to new technologies such as electronic surveillance).

126. California leads the charge in privacy legislations, passing comprehensive data privacy legislations such as the Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and the California Online Privacy Protection Act (CalOPPA). While some states have passed similar legislation, the vast majority of states still lack any kind of meaningful data privacy laws. *See State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEG. (Feb. 25, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (finding that only California, Nevada, and Virginia have enacted comprehensive consumer data privacy laws).

127. The primary tort laws that offer privacy protections are the intrusion upon seclusion and the public disclosure of private facts. However, both of these protections are very narrow, and as such, the plaintiff is unlikely to prevail in most circumstances. The intrusion upon seclusion tort applies only when the intrusion is "highly offensive" to a reasonable person. Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N. C. L. REV. 991 (1995). Additionally, this tort is not applicable when the plaintiff is in an area accessible to the public. *Id.* at 991–92. The public disclosure of private facts is often outweighed by the defendant's free speech interests, leading some scholars to declare this disclosure tort "all but dead." Jonathan B. Mintz, *The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain*, 55 MD. L. REV. 425, 448 (1996); *see also* Florida Star v. B.J.F.**,** 491 U.S. 524 (1989) (holding that a newspaper could not be held liable to a rape victim for violating a state law by printing the victim's name without the victim's consent because the newspaper lawfully obtained the victim's name from a police report).

128. *See, e.g.*, LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1224, 1227, 1237 (2018) (holding that the FTC needs greater specificity in its consent orders to provide "fair notice" for enforcement).

personal data by public actors such as the United States security agencies."[129] This reinforces the administrability and enforcement concerns regarding international data privacy agreements, as denoted in Part I.

Finally, the Safe Harbor Agreement suffered from complex jurisdictional procedures. In *Schrems I*, following Edward Snowden's 2013 revelations around National Security Agency ("NSA") practices,[130] Maximillian Schrems, an Austria citizen residing in Austria, filed a complaint against Facebook with the Irish DPC.[131] He alleged that the United States does not provide adequate data protection safeguards for EU citizens.[132] While the Irish High Court agreed that the NSA's actions demonstrated a "significant overreach" that compromised Europeans' data protection rights, the court nonetheless held that EU citizens do not have the right to be heard.[133] This is because the Irish law was effectively pre-empted by EU law, specifically by provisions of the 1995 Directive and the 2000 Decision establishing the Safe Harbour regime."[134] As long as the European Commission determined that the United States does provide an adequate level of data protection, then any complaint concerning the transfer of personal data on the grounds that the U.S. data protection regime is inadequate would be "doomed to fail."[135]

Schrems then appealed the case to the Court of Justice of the European Union (CJEU), which finally declared the Safe Harbor decision as invalid.[136] While this was ultimately a victory for Schrems and his fellow data privacy

129. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:627, ¶ 207 (Sept. 23, 2015).

130. In June 2013, Edward Snowden, a former CIA contractor, leaked information that the U.S. National Security Agency conducted a mass surveillance program, in which it collected the telephone records of tens of millions of Americans by tapping directly into the servers of nine internet firms (including Facebook, Google, Microsoft, and Yahoo). *Edward Snowden: Leaks That Exposed US Spy Programme*, BBC (Jan. 17, 2014), https://www.bbc.com/news/world-us-canada-23123964.

Following Snowden's revelations, ten of the world's largest human rights organizations launched legal challenges in Europe's top human rights court. Ryan Gallagher, *Europe's Top Human Rights Court Will Consider Legality of Surveillance Exposed by Edward Snowden*, THE INTERCEPT (Sept. 30, 2016, 1:13 PM). The European Parliament also launched an inquiry into the matter, in which it called upon the EU Commission to "immediately take necessary measures to ensure that all data transferred to the US [be] subject to an effective level of protection that is essentially equivalent to that guaranteed in the EU" because the U.S. surveillance practices encroached upon citizens "fundamental rights". European Parliament Press Release 20151022IPR98818, Mass Surveillance: EU Citizens' Rights Still in Danger, Says Parliament (Oct. 29, 2015), https://www.europarl.europa.eu/pdfs/news/expert/2015/10/press_release/20151022IPR98818/20151022IPR98818_en.pdf.

131. One of the interesting jurisdictional components of the GDPR is that it allows Schrems, an Austrian citizen, to file his complaint in Ireland. The broad territorial scope of the GDPR can lead to forum shopping, as discussed in Parts II and III.

132. *Schrems*, ECLI:EU:C:2015:627, ¶ 25.

133. *Id.* ¶ 35.

134. *Id.* ¶¶ 33, 41.

135. Schrems v. Data Prot. Comm'r [2014] 2 ILRM 441, ¶ 80 (H. Ct.) (Ir.).

136. *Schrems*, ECLI:EU:C:2015:627, ¶ 237.

advocates, it also revealed how pivotal and complex jurisdictional issues can be for international data privacy agreements.

B. *Safe Harbor as Game Theory*

To better understand the underlying incentive structures for the United States and the EU, this Note applies a game theory approach to the Safe Harbor Agreement. Each party can choose to either cooperate or to not cooperate with the terms of the agreement. This would leave the following 2 x 2 matrix with four potential outcomes. For each of the figures below, the best to worst outcomes are represented by the numbers four through one in descending order, with four being the best outcome and one being the worst outcome. The EU values are represented by the first number, and the U.S. values are represented by second number.

	United States		
European Union		Comply	Not Comply
	Comply	(4, 3)[137]	(2, 4)
	Not Comply	(1, 1)	(3, 2)

1. Assigning Values

In order to assign values to each potential outcome, this Note assumes the following value judgments. There are three core values at play: (i) national security; (ii) data privacy protections; and (iii) international legitimacy. National security and data privacy protections are competing interests locked in a zero-sum game. This is because if the government has greater access to individual data, then it could have more capability to prevent future crime and vice versa. International legitimacy is defined here as whether a government abides by its commitments.[138] Since the EU and the United States are both repeat players, if they violate a prior commitment, this makes other countries

137. This state is known as the Pareto-Optimal state because it is a state where no economic changes can be made to make one player better off without making the other player worse off. *See* Mike Shor, *Pareto Optimal*, GAME THEORY (Aug. 15, 2005), https://www.gametheory.net/dictionary/ParetoOptimal.html.

138. *See generally* Ian Hurd, *Legitimacy and Authority in International Politics*, 53 INT'L ORG. 379 (1999) (discussing the factors motivating a state to obey its commitments to uphold legitimacy in international relations).

more wary of entering into future agreements with them and vice versa. Finally, to assign the payout in each outcome, these values are weighed against each other in a balancing test, where greater weight is attached to certain values over others depending on the player.

Since the EU views data privacy as a fundamental and unalienable human right,[139] it can be assumed that this is their top priority, above both national security and international legitimacy. Next, since the EU considers itself and is also considered by others to be the de facto leader and standard setter in data privacy,[140] it has a strong incentive to uphold international legitimacy. Further, since data privacy protections and national security are locked in a zero-sum game, by prioritizing the former, it necessarily entails sacrificing the latter. As such, it can be assumed that with respect to data privacy issues, the EU prioritizes its international legitimacy over its national security. With these assumptions in mind, the EU's best outcome is in the top left box, where both the United States and the EU comply with the Safe Harbor Agreement. This is because this outcome meets all three core values for the EU. The EU's next best outcome is the bottom right box, where neither party complies with the agreement. Here, while the EU's top priority of data privacy protections are not met, the other two values are met, since the EU is not risking the transfer of sensitive data into the hands of the U.S. government, and the EU is not breaking the agreement in bad faith. The EU's third best outcome is the top right box, where the EU complies with the agreement, but the United States fails to comply. Here, the EU is only able to meet its value of international legitimacy since it followed through with its compliance commitment. The worst outcome is the bottom left because it undermines the EU's top two priorities. Here, by failing to abide by its own data protection principles, EU regulators are not protecting individual data rights and also risks undermining its reputation as the leader in data privacy.[141]

From the Snowden revelations, it can be assumed that the United States prioritizes its national security interests above both data privacy protections and international legitimacy. This is further supported by the *Schrems I* holding where the CJEU found that the U.S. national security and law enforcement requirements have "primacy" over the Safe Harbor principles.[142] With this assumption, the United States' best outcome is the top right box, where the United States does not comply with the Safe Harbor Agreement but the

139. *See* Part I.A.

140. *See, e.g.*, Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. Rev. 771, 772 (2019) (referring to the EU as the "world's privacy cop").

141. For the EU, the bottom left box reflects a worse outcome than the bottom right box because the former fails two of the three values, whereas the latter only fails one of the values. Although the former may provide slightly more data protection than the latter since there at least the United States is adhering to data protection principles, this slight difference is not enough to outweigh the loss of two core values.

142. Weiss & Archick, *supra* note 115, at 7.

EU does comply. Here, the U.S. government gets the most amount of data possible, thereby maximizing its national security interests, while still reaping the agreement's economic benefits. The United States' next best outcome is the top left box where both parties comply with the agreement. Here, while the United States does not maximize its national security benefits, it does fulfill the two other values by following through its data protection commitments. Since the EU complies with the agreement in this scenario, there is less risk that sensitive U.S. citizens' data will be compromised, thereby safeguarding U.S. national security interests. The United States' third best outcome is the bottom right box where neither party complies with the agreement. Here, while the United States fails to secure an international agreement and loses its economic benefits, it is at least able to prevent its sensitive data from being shared with the EU, thereby protecting its national security. The United States' worst outcome is the bottom left box where it complies with the agreement, but the EU does not. Here, the United States is exposing its sensitive data to potential misuse by the EU authorities, thereby severely undermining U.S. national security interests.

2. Application[143]

From the outset, the United States maintains a dominant strategy to not comply. This is because regardless of whether the EU chooses to comply or not comply, the United States would always receive a better payout by choosing to not comply.[144] In contrast, the EU has a reactive strategy, since its optimal choice is contingent on whether the United States chooses to comply.[145] In a static game where both parties cannot stray from their initial decision to comply or not comply, if the United States adheres to its dominant strategy, then the game would end at the bottom right box, since the EU's optimal response is to retaliate in kind.

However, in real life, the parties can shift their choices based on changing circumstances and strategize accordingly. Such shifts transform the static

143. The following application is inspired by the Theory of Moves, a game theory technique first endorsed by Professor Steven Brams. *See* Steven J. Brams, *Theory of Moves*, 81 AM. SCIENTIST 562 (1993).

144. For example, assume that the EU chooses to comply. This would lock the game into the top row, where the United States is faced with a payout of either 3 (where the United States chooses to comply) or 4 (where the United States chooses not to comply). Now assume that the EU chooses to not comply. This would lock the game into the bottom row, where the United States is faced with a payout of either 1 (where the United States chooses to comply) or 2 (where the United States chooses to not comply). In either scenario, the United States would always have a better payout to not comply.

145. If the United States chooses to comply, then the EU's optimal choice is also to comply. However, if the United States chooses to not comply, then the EU's optimal choice is to respond in kind and also not comply.

game into a fluid game.[146] When the Safe Harbor Agreement was first signed, both parties agreed to comply with its principles, thus starting the game at the top left box. While the EU has no incentive to change its position because it is already in its optimal state, the United States does have an incentive to shift to non-compliance as the shift would result in the United States' optimal state (i.e., the top right box). This is also exactly what happened, since the NSA decided to break its Safe Harbor principles by implementing a secret, mass surveillance program.[147] However, once the United States shifts to non-compliance, the EU now also has an incentive to shift to non-compliance based on its reactive strategy, resulting in the bottom right box. In this state, the United States has no incentive to shift back into compliance (i.e., moving from bottom right box to bottom left box), as that would result in the United States' worst outcome. Similarly, the EU has no incentive to revert back to compliance, as such a shift would yield a worse payout. As such, the bottom right box where neither party complies with the agreement is the Nash Equilibrium state,[148] and where the game ultimately ends.

This closely reflects how the Safe Harbor Agreement broke down in actuality. Shortly after the Snowden revelations, Maximillian Schrems filed his complaint, leading the CJEU to strike down the agreement altogether.[149] It is important to note that the efficiency of the fluid game is contingent on the parties' ability to detect defection. For example, if the EU failed to detect that the United States defected to non-compliance, then due to the informational asymmetry, the EU would not be incentivized to shift its position. Such detection in the real world, however, is not always apparent or immediate. This perhaps explains why the United States was keen to keep its surveillance program a secret, as it understood that this program would jeopardize the agreement, resulting in the inferior Nash Equilibrium state.

IV. APPLYING POTENTIAL SOLUTIONS

This Part proposes three potential solutions to overcoming the various obstacles impending an international data privacy agreement: (i) attaching data transfer requirements to trade agreements; (ii) applying discretionary

146. A fluid game still incurs some costs associated with shifting from one outcome to another. For example, if a party shifts from compliance to non-compliance, it incurs reputational costs as such a move undermines international legitimacy. If a party shifts from non-compliance to compliance, then it incurs administrative and transaction costs (i.e., compliance costs). For the purposes of this Note, the impact of these costs on the overall payouts and the decision-making process are presumed to be negligible.

147. *See* Part III.A.

148. Nash equilibrium is a concept of game theory where the optimal outcome of a game is a state where no player has an incentive to deviate from their chosen strategy after considering an opponent's choice. James Chen, *Nash Equilibrium*, INVESTOPEDIA (Mar. 3, 2021), https://www.investopedia.com/terms/n/nash-equilibrium.asp.

149. *See* Part III.A.

enforcement and rating systems; and (iii) allowing extraterritoriality to promote "race to the top" standards.

A. *Data Protection Principles as Pre-Requisite Conditions for Trade Agreements*

When negotiating trade deals, countries can tie data protection principles as a pre-requisite condition for the trade agreement to be implemented. So long as the economic benefits outweigh the potential downsides of implementing data privacy protections (e.g., administrability and enforcement costs), then it is rational for a country to comply with the terms of the data privacy agreement. As an example, the United States-Mexico-Canada Agreement (USMCA) required all parties to have a legal framework to protect personal information, have consumer protection laws for online commercial activities, and not prohibit or restrict cross-border transfer of information before the agreement could be implemented.[150] Similarly, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTTP/TPP-11), entered among eleven Asia-Pacific countries, required all parties to adopt a legal framework that provides protection of personal information for the users of electronic commerce.[151]

The game theory analysis in Part III helps understand why such an approach can be appealing. By attaching data privacy protections as pre-requisite conditions for the agreement to be implemented, the EU starts the game in its non-compliance state. By being unwilling to comply unless the United States also complies, the EU is no longer a reactive party but rather a proactive party, forcing the United States to choose between bottom row outcomes (its two worst outcomes), or the pareto-optimal outcome (top left box). By issuing this compellent threat, the EU can force the United States to divert from its dominant strategy of non-compliance. Alternatively, if the financial considerations significantly outweigh other competing values, then the parties' value judgments in the 2 x 2 matrix would also change. For example, if economic prosperity outweighed national security concerns in the United States, then perhaps the United States' best outcome would also be to comply.

However, attaching data privacy protections to trade agreements can be a risky move. While the agreement is in limbo, billions of dollars may be at

150. United States-Mexico-Canada Agreement ch. 19, July 1, 2020, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.

151. Comprehensive and Progressive Agreement for Trans-Pacific Partnership art. 14.8, Mar. 8, 2018, https://www.mfat.govt.nz/assets/Trade-agreements/TPP/Text-ENGLISH/14.-Electronic-Commerce-Chapter.pdf; *see also Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)*, AUSTRALIAN GOV'T DEP'T OF FOREIGN AFFS. & TRADE, https://www.dfat.gov.au/trade/agreements/in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership (last visited Apr. 19, 2022).

risk.[152] Furthermore, such aggressive postures could worsen geo-political relations between countries, making it less likely that they will come to an agreement in the future. Finally, there is no guarantee that countries will actually comply in good faith, as seen when the United States deviated from the Safe Harbor Agreement.[153]

B. *Discretionary Enforcement Mechanisms & Rating System*

Countries can implement a discretionary enforcement mechanism, where national regulators can choose both *what* to enforce and *who* to enforce against.

What to enforce refers to the national regulators' ability to choose which data privacy principles to adopt into their own legal regimes.[154] Depending on how many of these principles are adopted and enforced, an international organization (e.g., the United Nations) or independent institution (e.g., the Information Security Forum) could then grade countries on their overall data privacy regime.[155] Countries with higher grades would be allowed to handle greater volumes of data and transfer more sensitive data abroad and vice versa.[156] However, the effectiveness of this system relies on at least two crucial factors. First, countries and organizations must be able to categorize its data accurately and efficiently, potentially incurring high administrability costs. Second, the grading system must be standardized and uniformly accepted. This could be difficult to achieve since countries have different conceptions of data privacy and may weigh certain principles (e.g., consent) more heavily than other factors (e.g., notice and choice).

Who to enforce refers to both the national regulators' ability to selectively enforce certain data privacy principles to certain groups of individuals (i.e., different enforcement for domestic nationals and foreign nationals) and the ability to designate which country's regulator is responsible for

---

152. *See, e.g.*, W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485, 506 (2020) (noting that without the Safe Harbor Agreement, roughly $120 billion in trade would be withheld between the United States and the EU).

153. *See* Part III.A.

154. This reflects the OECD Guidelines approach, where each member state is free to choose which of the articulated general principles they wish to adopt in their own legal regime. *See* Part II.C.

155. The Information Security Forum (ISF) has introduced data privacy standards within its security assessments. The ISF Benchmark allows organizations to compare and measure their security systems against similar anonymous organizations around the world as well as against six internationally recognized standards. *The ISF Benchmark*, ISF, https://www.securityforum.org/solutions-and-insights/the-isf-benchmark-and-benchmark-as-a-service (last visited Apr. 21, 2022).

156. China already suggested this type of tier-classification system in its PIPL. Under Section II, organizations handling *sensitive* personal information must have additional procedural safeguards. Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), arts. 28–32 (China).

enforcement. With respect to the former, regulators could choose to apply two parallel systems of enforcement—one for domestic data subjects and one for foreign data subjects. For example, under the Safe Harbor Agreement, U.S. companies only needed to "apply Safe Harbor Principles to the personal data of Europeans" while retaining the discretion as to whether to also apply these standards to U.S. citizens as well.[157] This gives parties significantly more flexibility in implementing data privacy regimes, as compliance takes a sliding scale approach rather than an all-or-nothing approach. With respect to the latter, the right to enforce such agreements could be delegated to each country's specific enforcement agency rather than a centralized agency. For example, the Privacy Shield agreement between the United States and the EU deputized U.S. institutions to enforce the interests of EU citizens, accompanied by EU oversight.[158] This could circumvent much of the complex jurisdictional issues while also maintaining each country's digital and national sovereignty. However, with greater flexibility and greater legal pluralism, the countries can share vastly different privacy regimes, leading to inconsistent applications and legal uncertainty—the very same issues that also plague the OECD Guidelines and the APEC CBPR.[159]

Despite these reservations, a flexible approach could prove particularly beneficial for developing countries. Consider, for example, a country (Country A) that lacks the economic and administrative resources to fully comply with the GDPR and is subsequently unable to meet the adequacy determination for cross-border data transfers. Since data transfers are the lifeblood of the digital economy, this determination may force Country A and its companies out of the EU market altogether. Without access to the EU market, Country A could be trapped in a vicious cycle since its slower economic growth leaves it with even fewer resources to adapt to evolving data privacy policies. However, through the proposed approach, Country A could start by just adopting a few data protection policies, allowing it to transfer limited types of data and opening the door for its companies to slowly trickle into the EU market. This way, Country A can grow its economy and has strong incentives to continue integrating more data privacy principles in its legal regime, so that its economy and its companies can expand.

C. *"Brussels Effect": Extraterritoriality & Race to the Top*

The "Brussels Effect" refers to a "race to the top" as multinational entities find it easier to adopt the most stringent data protection standards worldwide rather than to satisfy divergent data privacy rules.[160] Countries with the

157. Schwartz & Peifer, *supra* note 8, at 159.
158. *Id.* at 176.
159. *See* Parts II.C & D.
160. The term is coined "Brussels Effect" because the rules and regulations "originating from Brussels have penetrated many aspects of economic life within and outside of Europe

largest market share have the most standard-setting power, since private companies in other jurisdictions with weaker standards are forced to either meet the higher standard or sacrifice a large portion of their exports.[161] This explains why the PIPL and the GDPR are so influential, as China and the EU occupy some of the largest markets in the world.

This approach circumvents the "harmonization" and coordination problems in reaching international data privacy agreements, since in theory, a country could unilaterally set the global standards (e.g., Chinese policymakers adopting the PIPL). Further, a single set of rules could allow for greater administrability, lower transaction costs, and fewer forum shopping concerns. However, the success of this approach is contingent on the country's ability to apply its laws extraterritorially. As denoted in Part II, extraterritoriality often undermines international comity, which can make it more difficult to reach future international agreements. Furthermore, countries may be rightfully hesitant in putting the rights of their own citizens in the hands and jurisdiction of another country. Finally, given the social, cultural, and personal significance of individual data privacy rights, it seems particularly questionable whether "might makes right" is the proper approach to determine the standard-setter.

V. CONCLUSION

As the modern world becomes ever-increasingly interconnected, it relies on a robust digital freeway, where big data can be safely and efficiently transferred across borders instantaneously. To facilitate such transfers, it is essential to define rules of the road by establishing international data privacy agreements. Yet the path to reaching such agreements is at a crossroads.

On the one hand, countries could work together to adopt a cooperative approach and set a universal data privacy framework. However, this approach faces significant headwinds from conflicting incentives and coordination problems, as illustrated with the collapse of the Safe Harbor Agreement. On the other hand, countries could adopt a unilateral territorialism approach where each country or region adopts its own data privacy regime. While this circumvents some of the coordination difficulties, it also leads to a fragmented global approach towards facilitating cross-border data transfers. This, in turn, would lead to a tragedy of the commons' situation where transaction

---

through the process of 'unilateral regulatory globalization' . . . Unilateral regulatory globalization is a development where a law of one jurisdiction migrates into another in the absence of the former actively imposing it or the latter willingly adopting it." Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 389 (2019).

161. *See generally* DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY (1995) (arguing that liberal trade policies can strengthen regulatory standards because powerful sectors of the economy with high regulatory standards will also drive up the regulatory standards of the rest of the economy); *see also* Petkova, *supra* note 113, at 1137.

costs for all countries are increased and international comity is undermined due to conflicting and overlapping jurisdictional authorities.

Policymakers are also faced with a difficult conundrum. By adopting stringent regulations, policymakers risk pricing out SMEs through increased compliance and administrability costs. This, in turn, could further entrench BigTech, giving them outsized influence over policymakers and consumers alike. However, by adopting overly lenient regulations, then individual data privacy rights may not be adequately protected, giving rise to national security concerns. Thus, policymakers must strike a delicate balance, one that offers both flexibility and proportionality in enforcement, such as those suggested in Part IV.

Fortunately, countries around the world have already made significant strides in cooperating, creating, and enforcing data privacy agreements as seen in Part II. While such agreements are not without their flaws, they represent a vision for a collaborative rather than divisive future—a digital new world.