EU DATA GOVERNANCE: PRESERVING GLOBAL PRIVACY IN THE AGE OF SURVEILLANCE

by
Nicola F. Daniel

A thesis submitted to the Johns Hopkins University in conformity with the requirements for the degree of Doctor of International Affairs

Baltimore, Maryland
December 2022

Abstract

The thesis explores the EU's Global Data Protection Regulation (GDPR), its human rights approach to data privacy, and its diffusion around the world. It asks the question: why would any nation, authoritarian or democratic, adopt Europe's data privacy framework as a model for their country's data governance? Accessing the theoretical frameworks of the Brussels Effect and the New Interdependence Approach, the research considers country case studies on China, Japan, and the US, comparing the different motivations and structural conditions that dictate how these three countries have adopted and adapted the GDPR framework. It finds a vastly different set of conditions for adopting the GDPR data privacy framework, none of which can be explained fully by either the Brussels Effect or the New Interdependence Approach. It also finds that none of the three countries embrace the language of human rights in their data privacy legislation. Of all the three countries, Japan has converged most closely with the GDPR in letter and spirit over time. While China's legislation bears all the key

features of the GDPR, the de facto reality is that data privacy regulation is a tool of state control. The United States case shows how a changing global environment forced the U.S. legislators to retreat from their market-driven approach to data governance in the direction of GDPR-like regulation.

Primary Reader & Advisor:	Matthias Matthijs, PhD
Secondary Readers:	Henry Farrell, PhD,
	Abraham Newman, PhD

Contents

Tables

Figures

Abbreviations

APPI	Act on the Protection of Personal Information Held by Administrative Organs, Japan's data protection law
CCP	Chinese Communist Party
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSL	Cybersecurity Law of the PRC
DPA	Data Privacy Authority
DPD	EU's 1995 Data Privacy Directive
DPO	Data Privacy Officer
DPP	Data Privacy and Protection
DSL	Data Security Law of the PRC
EC	European Commission
ECHR	European Convention on Human Rights
ECJ	European Court of Justice, formally called the Court of Justice of the European Union (CJEU)
EU	European Union
FTC	Federal Trade Commission
GDPR	Global Data Protection Regulation
GFC	Global Financial Crisis (of 2008)
NIA	New Interdependence Approach
PIPL	China's Personal Information Protection Law
SCCs	Standard Contractual Clauses
TFEU	Treaty on the Functioning of the European Union
TPP	Trans-Pacific Partnership
UNCTAD	United Nations Conference on Trade and Development

1 Chapter I: Overview

1.1 Introduction

Beijing, 1992, by Nicholas D. Kristof, *New York Times International:*

> *"Behind a locked metal grill door on the second floor of the Beijing Engineering Design Institute is a small room stacked with files from floor to ceiling. There is a file here on each of the institute's 600 employees, and although they are never allowed to peek inside, they live all their lives with their files looming over them. As part of China's complex system of social control and surveillance, the authorities keep a dang'an, or file, on virtually everyone except peasants. Indeed, most Chinese have two dang'an: one at their workplace and another in their local police station.*
>
> *A file is opened on each urban citizen when he or she enters elementary school, and it shadows the person throughout life…. Particularly for officials, students, professors, and Communist Party members, the dang'an contain political evaluations that affect career prospects and permission to leave the country.*
>
> *The file system in China is fundamentally different from any in the West, not only because the Chinese system encompasses all urban citizens, but because the file is kept by one's employer. The dang'an affects promotions and job opportunities, and it is difficult to escape from because any prospective employer is supposed to examine an applicant's dang'an before making a hiring decision. And there is no Freedom of Information Act to allow access to material in one's file.*
>
> *From a Chinese perspective, the absence of a comprehensive system of national files is one of the most perplexing lapses of American society, like the inability of New York to curb graffiti or narcotics. In China, which has a 3,000-year history of bureaucratic controls and no tradition of privacy—not even a good way of expressing the idea in the Chinese language—virtually nobody seems upset about the presence of the dang'an system."* [1]

What makes data protection one of the central debates of our time? We live in the age of the digital dossier, the 21st-century equivalent of the *dang'an (档案)*, where exabytes of

[1] NICHOLAS D. KRISTOF, "Beijing Journal: Where Each Worker Is Yoked to a Personal File," *The New York Times* (New York), March 16, 1992.

data about people flow across companies, governments, social media platforms, and borders—most of it without the data subject's knowledge.[2] The 1992 anecdote from Nicholas Kristof illustrates the coercive power of information aggregated about individuals—even in the archaic form of paper. Citizens in democratic societies struggle to grasp the scope and scale of data gathering and, more importantly, the attendant consequences in their daily lives. In an ironic twist, Kristof's article described how Chinese citizens felt the *dang'an* was becoming increasingly irrelevant as China took baby steps in its short-lived experiment with a more open and liberal society. It describes individuals who started their own businesses to circumvent the Chinese Communist Party (CCP) employment apparatus or had their files transferred to private staffing agencies that would allow them to be free agents in China's fledgling private sector. The article concludes that the diminishing relevance of the *dang'an* explained Chinese citizens' indifference to it during that window of China's Reform and Opening Up (改革开放).

However, new technologies have changed China, like the rest of the world. The *dang'an*—now in digital form—has not only reasserted itself with a vengeance in China but has also inserted itself into liberal and open societies in ways that undermine their very foundations. In the US, companies have gathered private data and monetized it under the guise of providing "free" services. The data thus aggregated has resulted in exceptional market power concentration that undermines competition, consumer choice, and ultimately innovation. Data and its (mis)use have become an important nexus of confrontation between democratic and authoritarian governments and all their varieties in between. Some, like Yuval Harari, argue

[2] An exabyte is an extraordinarily large unit of digital data. One exabyte (EB) is equal to 1,000 petabytes or one billion gigabytes (GB). Some technologists have estimated that all the words ever spoken by mankind would be equal to five exabytes.

that today's technologies favor autocrats. China's ability to collect data without restraint gives it an edge over the West in artificial intelligence and other emerging technologies, many argue.[3] China's totalitarian turn makes the images of George Orwell's Big Brother or Jeremy Bentham's panopticon popular metaphors promoted in the West's image of China. [4] The European Union has vigorously inserted itself into the panopticon by imposing aggressive regulation on companies that would do business with EU citizens. In doing so, they take seriously a core issue raised by Harari in his dystopic essay, "Why technology favors Tyranny":

> *"There is nothing inevitable about democracy. For all the success that democracies have had over the past century or more, they are blips in history. Monarchies, oligarchies, and other forms of authoritarian rule have been far more common modes of human governance.*
>
> *The emergence of liberal democracies is associated with ideals of liberty and equality that may seem self-evident and irreversible. But these ideals are far more fragile than we believe. Their success in the 20th century depended on unique technological conditions that may prove ephemeral."*[5]

1.2 Thesis Topic

The topic of this thesis is the EU's effort to achieve cross-border sharing of private data that creates the conditions for trust and innovation in an interdependent global economy. More narrowly, this thesis looks at the European Union's (EU) Global Data Protection Regulation (GDPR), its human rights approach to data privacy, and its diffusion worldwide. It asks the

[3] Bruce Schneier, *The Coming AI Hackers*, Belfer Center, Harvard University (2021), https://www.belfercenter.org/publication/coming-ai-hackers.

[4] A panopticon is a theoretical type of institutional building and system of control designed by the English philosopher Jeremy Bentham in the 18th century. The concept of the design is to allow all inmates of a prison to be observed by a single monitor or security guard. Although it is physically impossible for a single guard to observe all prison cells at once, the fact that the inmates cannot know when they are being watched at any given moment theoretically motivates them to act as though they are being watched at all times. Thus, the inmates are compelled to regulate their own behavior.

[5] Yuval Harari, "Why Technology Favors Tyranny," *The Atlantic*, no. October 2018.

question: why would any nation, authoritarian or democratic (or some variety of either), adopt Europe's data privacy framework as a model for their country's data governance? The thesis highlights the EU's role as a superpower in global regulation writ large but looks at this role specifically through the powerful lens of data flows. Europeans have been successful in promoting their vision of data governance to a significant degree; as demonstrated in the language adopted by the UN Conference on Trade and Development (UNCTAD) in a quote from its *Digital Economy Report 2021*, "Data are multidimensional, and their use has implications not just for trade and economic development but also for human rights, peace and security. Responses are also needed to mitigate the risk of abuse and misuse of data by States, non-State actors, or the private sector."[6] The language of this quote bears the strong imprint of EU thinking. As noted by Bruno Gencarelli, the European Commission's chief data privacy negotiator, "Europe was early in its recognition of data privacy as a global issue…If anything, the biggest effect of the GDPR is that it has created a culture of enforcement."[7]

The EU's leadership role has its challengers. Both the United States and China have resisted EU frameworks. The former has accused Europe of protectionism instead of data protection, and the latter assumes the European nomenclature even as it passes some of the most draconian data flow restrictions in the world under the banner of "cyber-sovereignty." The case studies in this thesis bear out this reality. To understand the sources of this resistance, we need to establish how, through the GDPR, the EU has sought to regulate personal data flows.

[6] UNCTAD, *Digital Economy Report 2021: Cross Border Data Flows and Development*, United Nations (Geneva, 2021).
[7] IAPP Europe Data Protection Congress Panel Discussion, November 2021.

1.2.1 What is the GDPR?

The GDPR is the EU's attempt to respond to the Big Data[8] age based on privacy principles that have been in place since the Organization for Economic Cooperation and Development (OECD) first created transnational guidelines on the transfer of personal data in 1980.[9] It is the culmination of an oft-contentious European dialogue between regulators, industry, and NGOs on how personally identifiable information should flow across international borders. It currently represents the most stringent global standard for individual data protection, with some notable exceptions like China, which has still more demanding standards. As a supranational regulation, it covers the 450 million residents of the EU and its 27 member nations. All EU member nations are bound to the standards; their enforcement occurs at the country level and requires member nations to revise their domestic laws to harmonize with the regulation. The GDPR frames data privacy and protection as a human right, a uniquely European approach with important consequences, as seen throughout this thesis. Indeed, privacy and data protection are enshrined in the EU Treaties and the EU *Charter of Fundamental Rights*, which serves as the EU's proxy constitution.[10] (See Appendix 1 for definitions and details of data, privacy, and human rights.)

The EU's first data privacy guideline, the Data Privacy Directive of 1995 (DPD), was motivated by the integration of the European economies into a Single Market and adopted the eight major principles of the original OECD guidelines. Ratified in 2016, the GDPR updates the rights

[8] For an excellent overview of Big Data and its varied definitions, refer to Amazon Web Services website introduction: "What is Big Data?," Amazon Web Services, accessed March 3, 2022, https://aws.amazon.com/big-data/what-is-big-data/. For a definition of data, see Appendix I.
[9] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (Paris: OECD, 1980).
[10] European Union, "Charter of Fundamental Rights of the European Union," (2012).

established under the DPD for the internet age and creates new citizen rights. These include the right to be forgotten and the right to data portability. Moreover, as a regulation rather than a directive, the GDPR is legally binding on all member nations once enacted and requires them to pass national-level laws to comply.

The thrust of the GDPR is to facilitate data flows while protecting consumers' information and allowing them the right to control who holds their information in commercial and certain government transactions. This is revolutionary from the consumer's perspective: the GDPR transforms an individual's exclusive status as a "data subject" to a broader understanding of the consumer as both data subject and data controller. Refered to as the *gold standard* of data protection regulation, many GDPR principles have been adopted in various forms by 120 countries.[11]

Without overplaying the analogy, the GDPR can be considered a regulatory equivalent of a data protection recipe or general-purpose technology (GPT).[12] A GPT is a "technology that initially has much scope for improvement and eventually comes to be widely used, to have many uses, and to have many … technological complementarities."[13] Examples of GPTs are the Gutenberg press, the steam engine, the computer, and electricity. Today, scholars increasingly refer to AI as the next GPT. The distinguishing features of GPTs include being highly innovative, easily adapted to various contexts, their applications eventually become widespread, they have

[11] Graham Greenleaf, Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 2018.
[12] Jonathan Keane, "From California to Brazil, Europe's privacy laws have created a recipe for the world," (April 8, 2021). https://www.cnbc.com/2021/04/08/from-california-to-brazil-gdpr-has-created-recipe-for-the-world.html.
[13] "What is General Purpose Technology?," ed. Maria Manuela Cruz-Cunha, Patricia Gonçalves, and Isabel Maria Miranda, *Handbook of Research on ICTs and Management Systems for Improving Efficiency in Healthcare and Social Care* (IGI Global, 2013).

a paradigm-shifting impact on economics and geopolitics, and their implications can take multiple implications generations to realize.[14] Within regulatory frameworks, there are good parallels between GPTs and the GDPR and its European predecessors. We are still in the early days of data governance, and many factors can still change the directional outcome. While it is clear that the GDPR has changed how governments think about data governance, what remains open-ended is the degree to which newer global data governance regimes at the country level will protect individuals against institutional abuse of their data. As noted by Newman, "political institutions provide the backbone for regulatory export."[15] Similarly, for adopting countries, political institutions are critical in adopting and adapting the regulatory framework to local conditions such that they become durable through enforceability. What can be said with certainty is that the GDPR stimulated the first-time adoption of data protection laws around the globe that broadly rely on the GDPR's nomenclature. In cases where data protection laws already existed, e.g., Argentina and Uruguay, the GDPR stimulated a trend toward upgrading and tightening standards around global data flows.

Earlier incarnations of EU data privacy laws focused on harmonizing data flow regulations to prevent firms from moving data to jurisdictions with lower standards.[16] The Cambrian explosion of data exchanges through newer technologies, including the internet, Smartphones, and social media, prompted regulators to turn their attention to personally identifiable

[14] For an extensive discussion of GPTs and their application in the international relations context, cf. Jeffrey Ding, *Stanford University HAI Seminar Series: The Rise and Fall of Great Technologies and Powers* (HAI Stanford University).
[15] Abraham Newman, *Protectors of Privacy* (Ithaca: Cornell University Press, 2008). Pg. 104. This notion is also supported by Jeffrey Ding, who argues that countries whose institutions are best able to support GPT adoption will be more likely to see their innovations used around the world.
[16] Newman, *Protectors of Privacy*.

information (PII). The GDPR represents the first comprehensive regulation for the Big Data era and is the subject of two core research questions.

1.3 Research Question

The puzzle that prompted this research was why China, an authoritarian nation, chose the GDPR as its data protection model. This question suggested a further one: why would any country adopt GDPR as a model? This research first intends to tell the story of how key aspects of the GDPR have been successfully transmitted in a series of country case studies on China, Japan, and the United States that highlight the confluence of factors leading to this outcome. To reiterate, the EU initially undertook data regulation largely for internal purposes. It had no explicit expectation of spreading its brand of data governance beyond the European Economic Community. Over time, however, the European approach gained currency globally, a fact that did not go unnoticed by EU officials. By 2006, the EU required each trade agreement it negotiated to include articles addressing data flows through which it sought to raise global data protection standards by leveraging the EU's market power. By 2016, the EU actively sought to externalize its principles through the GDPR and beyond.

Second, this research explores the limits of the GDPR and the degree to which the EU has been able to export data protection rules that encompass the human rights imperative so central to the European value framework. To do this, this thesis first shows how the broader human rights objective is achieved within the EU in the specific context of the digital economy. The EU's original mission to address the protection and privacy of personally identifiable data has evolved into a comprehensive project encompassing market competition and industrial policy. This establishes a comparative framework through which to evaluate third-country

adoption. China has recently completed its national digital strategy and is currently operationalizing it. Similarly, India started to address data protection legislation in 2019. That effort has since morphed into a far larger digital economy project comprising manifold issues, including personal and non-personal data, a vast shift toward greater data localization, and government-compelled access to private sector data. Countries large and small, developed and developing, are now engaged in data governance policy-making around the globe.

Although this research sets the EU as the benchmark for comparison, it by no means implies that its model should be the gold standard. Like all regulatory frameworks, it has features that impede its adoption in different contexts. For example, the insistence on human rights as a legal basis does not always translate well into other countries whose legal systems either protect them in different modalities, as is arguably the case of the US, or who subordinate human rights to other policy objectives, as in the case of China. Second, there is much valid debate over whether regulatory features like requiring firms to notify consumers how their data is being used, obtaining consumer consent to use that data, and mandating data portability are fit for the 21st century. While they offer consumers greater control over their digital dossier, do they really achieve the goal of protecting privacy? The latter debate is unlikely to see a definitive resolution.

This thesis has a comparative objective. It considers various theories of regulatory diffusion and relates them to the case studies, but it does not seek to produce a general theory of data privacy regulation diffusion. Besides the GDPR, there are other transnational instruments and mechanisms that seek to raise global data privacy and protection standards worldwide. These include, among others, the Council of Europe's Convention 108 and 108+, voluntary

commercial privacy codes, the African Union Convention, the Standards for Personal Data Protection for Ibero-American States with Latin American signatories, and the Asia-based APEC Cross-Border Privacy Rules system. The GDPR, however, has gained the most attention around the globe in part due to its extraterritoriality feature. This feature requires firms and governments to protect EU-generated data not just on EU soil, but also when transferred overseas, and they must do so in a fashion that complies with the EU's *Charter of Fundamental Rights*.

1.4 Theoretical Framework

The data protection debate is embedded within a wider theoretical discussion surrounding globalization, regulatory diffusion, and convergence. Second, it is located within a deep tradition of scholarship that evaluates the EU as an entity with the ability to project power globally despite its ambiguous status as neither state nor as an international organization.[17] Finally, it is embedded in theoretical discussions of the meaning of privacy, which are interpreted differently in alternate settings.[18] None of these distinct areas of scholarship maps neatly onto the other. This thesis focuses largely on the first and second discussions. This chapter refers to the second in the context of how the EU operationalizes its ability to project core European values outside its borders as a defensive exercise against the encroachment of external values that challenge its hard-won and somewhat fragile European identity. In the case of data privacy, the

[17] See Kathleen McNamara, "European Foreign Policy," in *The Politics of Everyday Europe* (Oxford: Oxford University Press, 2015). See also Kathleen R. McNamara, "Authority Under Construction: The European Union in Comparative Political Perspective," *JCMS: Journal of Common Market Studies* 56, no. 7 (2018), https://doi.org/https://doi.org/10.1111/jcms.12784, https://onlinelibrary.wiley.com/doi/abs/10.1111/jcms.12784.

[18] Cf., among many, Colin J. Bennett, "The privacy advocates : resisting the spread of surveillance," (Cambridge, MA :: MIT Press, 2008). https://doi.org/10.7551/mitpress/7855.001.0001?locatt=mode:legacy.; J. Fairfield and C. Engel, "Privacy as a Public Good," in *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* ed. R. Miller (Ed.) (Cambridge: Cambridge University Press, 2017).; Ari Ezra Waldman, *Privacy as Trust: Information Privacy in an Information Age* (Cambridge: Cambridge University Press, 2018).

core value is chiefly defined by the EU's obligation to protect the individual citizen from state or corporate overreach into the private sphere. Because of this, the thesis considers privacy and data protection definitions through European eyes and largely leaves aside the discussion of privacy in other cultural contexts. (Appendix 1 discusses definitional terms of data privacy and protection, privacy concepts, and human rights.)

The diffusion debate comprises dominant schools of thought that historically emphasize the state's role as the prime mover of regulatory change. The theories break down into explanatory frameworks that emphasize the following: 1) countries align and collaborate according to their preference for open economic exchange as against relatively more protectionist countries roughly in line with the neoliberal tradition/liberal institutionalism; 2) regulatory "race to the bottom," in which large multinationals leverage their size to coerce governments into weakening regulatory control by threatening to move production from their home country to a market overseas; [19] 3) market power theories that explain the transformation in terms of the dominant economy being able to force regulatory changes on other countries as a condition of market access, and;[20] 4) the interaction of domestic and international institutions, with some authors challenging the distinction between domestic and international in a globalized world and others

[19] This is sometimes referred to as regulatory arbitrage and has been theorized as the Delaware Effect. It refers to the ability of firms to incorporate in jurisdictions with lower regulatory standards even if their main business is conducted elsewhere. The globalized version of regulatory arbitrage is discussed in Thomas Oatley, "The Reductionist Gamble: Open Economy Politics in the Global Economy," *International Organization* 65 (2011). There is a related strand of theory that describes firms as increasingly supplanting the role of the regulators, sometimes unexpectedly resulting in raised standards. See Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton, NJ: Princeton University Press, 2011). See also Damien Geradin, Dimitrios Katsifis, and Theano Karanikioti, "Google as a de facto privacy regulator: analysing the Privacy Sandbox from an antitrust perspective," Article, *European Competition Journal* 17, no. 3 (2021), https://doi.org/10.1080/17441056.2021.1930450.

[20] Daniel W. Drezner, "All politics is global : explaining international regulatory regimes," (Princeton, N.J.: Princeton University Press, 2007). http://www.loc.gov/catdir/toc/ecip0615/2006017741.html.

arguing that domestic preferences are aggregated and subsequently represented in international fora. Although the lines are not always bright, these theories emphasize a static theoretical explanation with change occurring through systems clash. Robert Putnam's two-level game theory represents an evolution from the stylized systems clash, allowing for greater variation in outcomes based on the strategic calculus of the participants.[21] A further framework borrows from complexity or information theories, which describe a dynamic, infinite game in which the rules of the game can change over time and participants oscillate between gaining and losing advantage over time.[22]

More recent schools of thought, including the Brussels Effect and the New Interdependence Approach (NIA), take a more differentiated view, focusing on variant sets of actors as drivers of regulatory change. These actors can strive for both convergence and divergence in regulatory models. The Brussels Effect argues that countries or firms willingly adopt the EU's regulatory standards voluntarily and independently of their relationship with the EU, thus driving toward convergence. The theory still emphasizes the role of the EU as a state actor, describing the EU as a "regulatory hegemon." However, it also reflects the role of businesses in affecting laws or voluntary standards as they seek to increase cross-border transparency and efficiency. The Brussels Effect directly challenges the "race to the bottom" theories. It also seeks a more nuanced understanding of the EU's power by looking at the limits of its leverage according to various industries. For example, in finance, where capital can flow freely across borders, the EU

[21] Robert D. Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization* 42, no. 3 (1988), http://www.jstor.org/stable/2706785.
[22] See, for example, Thomas Oatley, "Toward a political economy of complex interdependence," *European Journal of International Relations* 25, no. 4 (2019).

has relatively less leverage through the Brussels Effect. In this case, the role of civil regulation, through which corporations agree to standards set by the private sector, can play a more dominant role.[23] However, the EU has higher standards-raising power in consumer food standards because food production often benefits from economies of scale that favor standardization of production processes across borders.

The NIA authors challenge the notion of the state as the key actor which reacts to global interdependence. Thus, they are theoretically related to current scholars like Thomas Oatley, who access complexity and information theory to explain international relations. They revive the work of Joseph Nye and Robert Keohane from the 1970s, who argued that the state is one among many actors integrated into a network of transnational actors.[24] These actors include policymakers, firms, and NGOs who meet to share knowledge and influence outcomes. The authors consider the iterative effects of regulatory diffusion through which, for example, a domestic regulatory change might have spillover effects in the international realm that result in second-order feedback to the domestic environment and vice versa. As such, globalization is seen as both the source and the result of domestic changes. The NIA looks at rule-overlap across borders and the network of non-state actors whose shifting opportunity structures reshape actor strategies and outcomes.

The thesis considers the Brussels Effect and the NIA through the empirical evidence of three countries: the United States, China, and Japan. It contends that the Brussels Effect has

[23] David Vogel, ""Private Regulation of Global Conduct"," in *The Politics of Global Regulation*, ed. Walter Mattli and Ngaire Woods (Princeton: Princeton University Press, 2009).
[24] Joseph S. Nye and Robert O. Keohane, "Transnational Relations and World Politics: An Introduction," *International Organization* 25, no. 3 (1971), https://doi.org/10.1017/S0020818300026187. For a more general discussion of the IPE intellectual tradition and the role of the state, see also Benjamin Cohen, *International Political Economy* (Princeton: Princeton University Press, 2008).

weak explanatory power in the case of large democratic countries like the US and Japan, while it has some explanatory power in the case of China. This finding is counterintuitive. One would expect that countries with shared democratic values would be more likely voluntarily to reference European data governance models given the EU's first mover advantage. Instead, the United States case is explained as a combination of the New Interdependence Approach and the Brussels Effect. In large part, this is because the NIA takes into account the power of coercion as a tool for defending or extending existing institutions, whereas the Brussels Effect does not.

In the China case, non-state actors have seen their participation in high-level policymaking increasingly circumscribed since Xi Jinping assumed power in 2012. As a result, a theory such as the NIA cannot explain China's adoption of GDPR principles. The Brussels Effect does—but only in the narrow sense of functioning as a legal template. Understanding China's approach to data governance must draw on an array of theoretical foundations. The Asia Crisis of 1997/98 and, more importantly, the Global Financial Crisis (GFC) of 2008 profoundly impacted China's leadership.[25] The GFC undermined the Chinese leadership's estimation of Western neoliberal economics and emboldened conservatives who had formidably resisted dismantling the state-owned sector. As a result, Dali Yang helpfully theorizes that China took a "Polanyian turn" to put guardrails on its Wild West economy.[26] At the same time, China's leadership was adjusting to the new world of the internet and the burgeoning wealthy, urban, and educated

[25]Barry Naughton, "China's Response to the Global Crisis, and the Lessons Learned," in *The Global Recession and China's Political Economy*, ed. Dali L. Yang (Palgrave Macmillan, 2012).
[26] Dali Yang, "China's Illiberal Regulatory State in Comparative Perspective," *Chinese Political Science Review* 2 (2017), https://doi.org/10.1007/s41111-017-0059-x.

"netizens" who took to social media to hold their local and central government bodies to account.[27] Information flows from the outside, and netizen activism from the inside threatened to undermine the CCP's domestic control of the narrative as well as images of China outside of the country. This phenomenon could lead to strong transnational ties to affect change, an NIA dynamic. The GFC, coupled with the empowerment of educated and insightful citizens who could challenge CCP orthodoxy and garner support through the Internet, proved to be a jarring test of the CCP's long-standing obsession with social stability. Just as the EU has developed the institutional will to combat the most pernicious effects of the digital economy through measures such as the Digital Services Act and the Digital Markets Act, China took on the task of building the institutional capacity to do the same in its domestic markets. China—like the EU—linked data governance to market regulation through its Polanyian turn.

Finally, the Japan case is best understood in the context of Shinzo Abe's grand strategy to transform Japan and to shore up its economic and national security interests, and thus neither the Brussels Effect nor the NIA capture the full dynamics at play. Japan adopted EU data privacy regulations as part of its quest to attain an EU data transfer adequacy finding. An EU adequacy finding allows third parties to transfer personally identifiable EU citizen data to servers located overseas and is increasingly critical to cross border trade in services and goods.[28] Abe saw data as a linchpin of global trade in the future and thus aspired to link data flows and trade flows in negotiations. Having granted one another *mutual adequacy* status in 2019, the EU-

[27] Elizabeth Economy, *The Third Revolution* (Oxford: Oxford University Press, 2018).
[28] An example of this would EU citizen data transmitted by cars imported to the EU from Japan to servers outside of the 27-member country region.

Japan collaboration on global data governance matters since that time suggests that the NIA may have taken over as the theoretical framework that best describes their interactions.

In sum, no single theory alone best explains how data privacy regulation manifests across global settings.

1.4.1 EU Push Factors

The common theme in all the case studies is that they each respond to the extraterritoriality requirement of the GDPR. The GDPR's territorial extension requires that entities who gather or process the information of EU citizens or residents cannot transfer data outside the EU unless the receiving jurisdictions have "essentially equivalent" legal protections for that data. How the EU interprets equivalency and how countries respond is a significant focus of inquiry in this thesis.

The long history that predated the GDPR created the conditions through which this extraterritoriality clause could gain purchase. The confluence of factors that played a salient role in Europe's data privacy diffusion is manifold, including timing, institution-building, EU internal subject-matter expertise on data flows, increasing global trade flows that proliferated in the 1990s, domestic factors in the adopting countries, and the EU's market size. These factors are logically linked as follows. First, when privacy issues pertained to the computer age first arose in the 1970s, there was a remarkably high level of harmony between the US and European attitudes towards data privacy that might have driven a global standard at that time. However, as shown by Abraham Newman, domestic factors in the United States generated resistance to an

independent privacy regulator in the US.[29] They thus resulted in the US's limited rather than comprehensive approach to data flow governance that has persisted until today.

Second, this US leadership gap opened a fissure for continental Europe to assume the mantle in global data governance along with a vast array of other policymaking opportunities, such as greenhouse gas emissions and food safety; among others. Already early on, three Europe-based institutions collectively addressed data flows across borders, including the Organization of Economic Cooperation and Development (OECD) in the 1980s, the Council of Europe (CoE), and the European Economic Community (EEC). These three institutions started the work of codifying and proliferating a European perspective on data privacy around the world.[30]

Third, when the Treaty of Maastricht came into force in 1992, the EU functionally replaced the EEC and galvanized two intense decades of institution-building. This project was guided by core EU values codified in the *Charter of Fundamental Rights of the European Union* and became legally binding in 2012. These institutions formed the vehicle through which the EU could project its power in the world and promote collective European interests. Initially, data flows were a secondary consideration in norms projection but assumed greater importance with the growth of the digital economy.

Fourth, the institution-building yielded a bureaucratic cadre with significant subject-matter expertise that it could leverage to nudge and sometimes to coerce European regional proliferation of higher data protection laws. This regional acceptance in the EU block increasingly exposed the EU's trading partners to those requirements and raised incentives to adopt

[29] Newman, Protectors of Privacy, 2008.
[30] Oliver Diggelmann and Maria Nicole Cleis, "How the Right to Privacy Became a Human Right," *Human Rights Law Review* 14, no. 3 (2014), https://doi.org/10.1093/hrlr/ngu014, https://doi.org/10.1093/hrlr/ngu014.

them. Fifth, as global trade flows exploded in the 1990s, the attractiveness of the European market added a lever through which regulators could tilt market behavior toward EU preferences, as Tim Wu and others argued.[31] Sixth and finally, the omnibus nature of the EU's regulations was intended to allow sufficient flexibility for the 27 member nations of the EU to adapt to their existing legal structures, as shown by Schwartz.[32] This was a crucial feature to cement data protection as a European culture and allowed for relative ease of adoption in third countries outside the EU.

1.4.2 Domestic Pull Factors

The above considered how the European Union projects its power, or the *push factors* involved in the diffusion of regulatory frameworks. Pull factors in each country's domestic dynamics also explain countries' relative willingness to adopt given regulatory standards. In Brazil, for example, the Edward Snowden revelations led to collaboration between then-Brazilian president Dilma Roussef and former German Chancellor Angela Merkel that resulted in a general resolution at the UN Human Rights Council recognizing that the privacy rights enjoyed by individuals offline should also apply online. Brazil's vibrant civil society actors were positioned to exploit the Snowden events to advocate for the strongest data protection framework in all of Latin America. In 2014, Brazil passed its *Digital Bill of Rights,* and in 2018, it further passed the *General Data Protection Law* (LGPD), which is in force today. The European model was adopted almost without consideration for alternatives, given the similarity of the underlying legal systems shared by Brazil and the EU, as noted by the author of Brazil's original draft data

[31] Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (Oxford University Press, 2006).
[32] Paul M. Schwartz, "GLOBAL DATA PRIVACY: THE EU WAY," *New York University Law Review* 94, no. 4 (2019).

protection law.[33] A second pull factor is exemplified in India's digitization of government campaign. India's introduction of a national biometric identification system in 2016 inspired a fractious national debate that saw privacy activists, lawyers, social justice advocates, government officials, and private sector market participants cooperating and competing to share or restrict access to data.

A third pull factor was globalization. Countries that were beneficiaries of globalization have also had compelling incentives to adopt data privacy regulation because of their desire to participate in the global economy in ways not conceivable until the fall of the Soviet Union. As the global economy increasingly digitized, the incentive to update data privacy rules was a function of the need to maintain economic and job growth to satisfy citizens' demands. The more dependent on trade a country is, the more likely it is to have put in place at least the basis of a data privacy regime.

Domestic factors also explain resistance to adopting GDPR rules. Two key requirements of GDPR legislation are independent data protection authorities not subject to political influence and a rejection of most data localization. These requirements have not been embraced in Asia for idiosyncratic reasons. China, for example, requires data localization in the context of its *cyber sovereignty* framework driven by national security perceptions and market competition motives. By contrast, in India, legislator calls for data localization is driven by industrial policy. For example, in 2019, India required all financial payment data to be stored locally. The localization requirement was an explicit drive to limit the role of foreign banks in the Indian market. A second example is India's aspiration to develop an indigenous cloud server industry. The top

[33] Danilo Doneda, "Expert Interview on Brazil Data Protection Law," interview by Nicola Daniel, February 22, 2022.

three players in the Indian cloud server market are Google, Amazon Web Services, and Microsoft. Indigenous Indian cloud service providers are a distant fourth and beyond. Indian legislators have thus explicitly embraced data localization to favor domestic players.[34] In sum, while domestic factors have heavily driven the adoption of European data protection rules, those same factors can also lead to limitations on the GDPR's full adoption.

1.5 Methodology

As the theoretical framework indicates, this work seeks to draw together a broad range of thinking and test it based on empirical observation. The variety of theoretical strands that this thesis relies on for explanatory power arose from research that included government documents, newspapers and think tank documents, the research output of industry bodies, podcast interviews with government officials and policy experts, conferences, and informally structured interviews with industry officials. In both the China and Japan cases, this research examined public government statements and translations of government documents. This thesis also relied on historical accounts and academic research that provided contextual framing and insight into the behavior of government officials, which could be applied in the data privacy and protection context. In the US case, this research accessed government officials' statements at US/EU working groups, roundtables, and panel discussions, some of which followed the Chatham House Rule for theoretical validation. The US case also reviewed legal academic literature to understand how the differing legal structures of the US and EU predisposed them to certain path dependencies.

[34] "Top 10 Cloud Providers in India," Back4App, accessed October 12, 2021, https://blog.back4app.com/cloud-computing-providers-in-india/.

Based on the initial research, the case study method appeared to be the most effective way to highlight the channels through which the GDPR found its way into third-country data governance regimes. To date, there are no quantitative studies that systematically address the adoption of GDPR rules globally. Frankenreiter studied nearly 700 privacy policies published by US firms using textual analysis and machine learning methods to read company websites. The study shows that very few US companies have comprehensively adopted GDPR-compliant rules. Instead, firms have segregated audiences across their web platforms, extending more strict privacy policies for EU citizens and more relaxed rules for US citizens. This finding thus undermines the Brussels Effect claim that one of the motives for adopting GDPR-compliant rules across global platforms is to achieve cost efficiencies.[35] While the study addresses the total number of firms, it does not evaluate the consumer reach of firmsthat have comprehensively rolled out the GDPR. One explanation for the lack of quantitative studies becomes clear in the case studies. Given the different adaptations of GPDR rules in local environments, it would be difficult to conduct quantitative analysis with sufficient like-for-like points of comparison. Even when local jurisdictions undertake wholesale adoption of the GDPR nomenclature, there are important differences in actual outcomes that would challenge the findings of a quantitative study. Studies of data protection issues, such as the number of data breaches or cost of data breaches per customer, lend themselves more readily to quantitative studies against data privacy and human rights outcomes.

[35] Jens Frankenreiter, "The Missing 'California Effect' in Data Privacy Laws," *Yale Journal on Regulation, forthcoming* (2021), https://doi.org/http://dx.doi.org/10.2139/ssrn.3883728.

The thesis covers three cases China, the US, and Japan, all of which showcase these differing pathways of GDPR transmission. The cases represent the biggest actors in global data flows. With the EU, they represent the world's four largest economies. They also reflect different forms of government, both authoritarian and democratic. These countries and the EU collectively represent those with the highest internet access and data consumption measured by per capita terabytes consumed.[36] In Big Data, countries with larger populations and greater economic power play an outsized role in determining data flows across borders. An OECD report on measuring the economic value of global data transfers cites one prediction that data flows will add $11 trillion to the global economy by 2025.[37] A study by McKinsey Global Institute relates data volume (or installed bandwidth) to economic value using regression analysis.[38] The three case studies in this thesis capture the vast majority of global economic value created by data inputs.

Brazil, India, and South Africa are three countries that might have been considered for this comparative study and are subjects for future research. Brazil and South Africa followed the GDPR closely when creating their data privacy legislation. India, as mentioned, is still debating its data governance regime. India's initial data privacy regulation proposed in 2018 was based significantly on the GDPR, though it has since retreated from the GDPR in important ways. Most recently, India withdrew its proposed data privacy legislation altogether. As with

[36] Bhaskar Chakravorti, Ajay Bhalla, and Ravi Shankar Chaturvedi, "Which Countries are leading the Data Economy?," *Harvard Business Review* (January 24, 2019). https://hbr.org/2019/01/which-countries-are-leading-the-data-economy.
[37] David Nguyen and Marta Paczos, "Measuring the economic value of data and cross-border data flows," (2020), https://doi.org/doi:https://doi.org/10.1787/6345995e-en, https://www.oecd-ilibrary.org/content/paper/6345995e-en.
[38] James Manyika and et al, *Digital globalization: The new era of global flows* (2016).

the three case studies in this thesis, Brazil, India, and South Africa show features of the Brussels Effect even as they highlight key limitations that the China case brings into relief.

1.6 Research Gaps

This thesis fills a gap in the literature on the GDPR in two ways. First, it compares three different modes through which the GDPR has spread and applies theoretical frameworks from the IR tradition that lend explanatory power. Given the rising importance of global data flows in generating economic growth, this initial effort is one upon which future comparative work can build. This research provides a cross-national approach to how individual nations have adopted and adapted aspects of the regulation. Other analyses of data regulation have occurred from a legal perspective, showing how the laws differ from country to country without considering the more broader political implications that play a role in data governance choices.[39] This is especially true in the Japan case study. Academic articles, by contrast, have focused on specific case studies documenting the effect of GDPR on particular industries, business models, or of the GDPR's adoption by given countries.

Second, it looks at the GDPR through the lens of the EU's ability to project and promote its values framework on the world. This is an important metric in the EU's self-defined vision. Graham Greenleaf has done a similar exercise for Asia completed in 2014, showing the limited impact of a human rights approach to data governance.[40] However, Asian standards have dramatically transformed since then – some convergent and some divergent from European

[39] See, for example, Christopher Kuner, "An international legal framework for data protection: Issues and prospects," *Computer Law & Security Review* 25, no. 4 (July 2009 2009).
[40] Graham Greenleaf, *Asian Data Privacy Laws, Trade and Human Rights Perspective* (Oxford: Oxford University Press, 2014).

standards. The case studies show that the specific human rights articulation has largely remained confined to Europe. That is, while countries broadly sign on to the *UN Charter on Human Rights* and the resolution affirming digital privacy rights, they do not embrace the language of human rights in their domestic data policy legislation.

Nevertheless, many countries have adopted certain key concepts, such as the data gatherer's obligation to notify and receive consent from an individual; the individual's right to access and correct information held by entities about them; the right to have their data deleted, and; the right to opt-out of receiving sales and marketing emails or texts. Adopting these measures into law with meaningful enforcement mechanisms *de facto* protects the individual from undue intervention in the private sphere in ways consistent with the EU's human rights conception of data privacy. Convergence on such standards is increasingly important in the current geopolitical environment. Democracies must share information through trusted frameworks to combat malign actors that seek to undermine the foundations of democracy, if not the current international liberal order itself.

1.7 Thesis Outline

This thesis pursues the following roadmap. Chapter 2 first discusses the EU's broader regulatory ecosystem for which the GDPR was the foundation. Second, it discusses important definitions and taxonomies central to the GDPR and describes its historical origin. This section is vital to laying out the basic landscape of an increasingly complex topic and a growing body of scholarly research. Finally, it places the GDPR in the context of the three major global approaches to data governance: that of the US, of the EU, and China. This comparison lays out a visual framework to orient the reader's understanding of the differences between the three

data governance regimes and how they pose challenges to global geopolitics in the digital economy.

Chapter 3 surveys the channels through which the GDPR is diffused. The chapter begins with a brief overview of competing transnational instruments used to facilitate cross-border data flows. The most important of these is the EU's adequacy status. Second, the chapter outlines the Brussels Effect and the New Interdependence Approach (NIA). These descriptions form additional building blocks for understanding the case studies.

Chapters 4 through 6 delve into the case studies. China is the first and is a particularly important case study. It is an example of the Brussels Effect in a very narrow sense that highlights the limits of that theory. China deeply studied the GDPR when it considered its new data protection law, the Personal Information Protection Law (PIPL), but ultimately passed its legislation without formal EU consultation. In essence, the GDPR became a legal template for China.

Nevertheless, China's use of the GDPR as a template is important because of the extremely high value the Chinese Communist Party (CCP) has placed on the digital economy as both a tool to legitimize its rule domestically and as a tool to project power globally. China adopted and adapted GDPR rules in 2021 as part of Chinese President Xi Jinping's massive drive to regulate and institutionalize the digitization of China's economy. In this sense, Xi continues the work started by Deng Xiaoping. Deng not only championed reform and opening up to the outside world (改革开放), but also initiated a groundbreaking and gargantuan effort to re-establish and update China's legal system after the Cultural Revolution.[41] While Xi is undoing the reform and opening up period in many formidable ways, his efforts to deepen China's

[41] Cf. Ezra Vogel, *Deng Xiaoping*.

regulatory system are entirely consistent with his predecessors. Data privacy laws support the goal of putting guardrails around China's market economy and building a national regulatory framework. By protecting individuals from excessive corporate data collection, privacy laws are as much tools to ensure the functioning of the socialist market economy as they are weapons to be used against China's largest entrepreneurial enterprises: Tencent, Alibaba, Baidu, Didi, Pinduoduo, and others. The recent anti-monopoly actions against these firms show how regulations are being used to legitimize government interference in China's market economy.

However, this is not the only motivation. Many Sinologists have characterized China's government as suffering from fragmented authoritarianism.[42] Fragmented authoritarianism accounts for how local and provincial governments inconsistently fulfill directives from the central government to meet their local needs, sometimes in passive defiance of central authority. If this is true, stronger data collection and regulation at the national level creates a mechanism to hold county and provincial level governments accountable. It helps to overcome what has been called the "dictator's dilemma" of not getting sufficiently accurate information to make sound governing decisions when subordinates seek to conceal truths that might not be palatable to authoritarian leadership.

Finally, although China preserved much of the framework of the GDPR, it has unsurprisingly subordinated the conception of privacy as a human right to the rule of the Communist

[42] Andrew Mertha, ""Fragmented Authoritarianism 2.0": Political Pluralization in the Chinese Policy Process," *The China Quarterly* Dec 2009, No. 200 (2009), https://www.jstor.org/stable/27756540., Kenneth Lieberthal, "Introduction: the 'fragmented authoritarianism' model and its limitations," in *Bureaucracy, politics, and decision making in post-Mao China*, ed. Kenneth Lieberthal and David M. Lampton (Berkeley :: University of California Press, 1992).

Party. China understands privacy differently than the West.[43] Yet, by using the Western human rights terminology and embracing data privacy regulations like the GDPR, China successfully co-opts the language of liberal democracies and creates semantic confusion. China has frequently and sometimes inconsistently argued that the right to development dominates human rights at this stage of China's development. [44] Understanding how China has articulated its stance towards human rights over time gives some insight into why adopting GDPR rules serves the government's larger objectives. In essence, signing on to Western-style privacy laws yet adapting them to suit Communist Party objectives is consistent with China's balance between participating meaningfully in the global system while seeking to rewrite its accepted norms simultaneously. By adopting GDPR-like privacy rules, China is following the same playbook as it has with the human rights narrative.

In this way, the GDPR provides a key example of how China's Communist Party is reinventing authoritarianism, Authoritarianism 2.0, in two ways. Domestically, it seeks to optimize rather than maximize its grip on its citizenry. In the face of pervasive surveillance, the ability of citizens to sue corporations for invasion of privacy gives them a sense of agency that may be just enough to ensure stability and ongoing single-party rule.[45] The core idea is that the adoption of Western-style GDPR rules reinforces rather than undermines party legitimacy. Internationally, China seeks to play by the rules and simultaneously change them.

---

[43] Rogier Creemers, "China's Emerging Data Protection Framework," (2021), https://doi.org/http://dx.doi.org/10.2139/ssrn.3964684.

[44] "Development as a human right : legal, political, and economic dimensions," ed. Bård-Anders Andreassen and Stephen P. Marks (Boston: Harvard School of Public Health, François-Xavier Bagnoud Center for Health and Human Rights, 2006).

[45] Francis Fukuyama, "The Origins of Political Order," (New York: Farrar, Strauss, Giroux, 2011). https://ebookcentral.proquest.com/lib/jhu/detail.action?docID=689270. Pg. 307.

The second case study is the United States. The US case is an example where both the Brussels Effect and the NIA explain elements of how the US gradually accepted EU data governance preferences. This case study unfurls the evolution of the EU-US data privacy relationship as a process through which the EU first conceded more than the US in striking data transfer agreements. When the Privacy Shield agreement was invalidated, a two-year period ensued in which something like the Brussels Effect dominated—that is, both firms and individual US states started adopting GDPR-like rules voluntarily and independent of their relationship with the European Union. California's 2019 data protection law is an example that closely mirrors the requirements and spirit of the GDPR. The newer version of California data protection law, the California Consumer Protection Regulation (CCPR), resembles the GDPR in all eight major areas. Four other U.S. states followed California in adopting comprehensive laws. Firms also began adopting GDPR rules across their global platforms. Microsoft's President, Brad Smith, famously rolled out GDPR principles across Microsoft's global platform and issued a *Global Human Rights Statement*.[46] The company now actively lobbies for enhanced data privacy regulation within the EU and US, following a pattern similar to that of US and European banks when the EU actively pursued greater integration into the global financial system during the 1990s.[47] Apple's CEO, Tim Cook, has also been a vocal advocate of data privacy regulations and has recently

[46] "Microsoft Global Human Rights Statement," https://www.microsoft.com/en-us/corporate-responsibility/human-rights-statement?activetab=pivot_1%3aprimaryr5.

[47] Refer to writings from Posner, including Elliot Posner, "Making Rule for Global Finance: Transatlantic Regulatory Cooperation at the Turn of the Millennium," *International Organization* 63:4 (October) (2009). See also Eric Helleiner and Stefano Pagliari, " Between the Storms: Patterns in Global Financial Governance, 2001-2007," in *Global Financial Integration Thirty Years On: From Reform to Crisis*, ed. Jasper Blom Geoffrey R.D. Underhill, and Daniel Mügge, eds. (Cambridge: Cambridge University Press, 2010).

used it as a competitive bludgeon against Facebook.[48] Today, major global firms cite the onerous resource cost of noncompliance to the GDPR and have subsequently pushed for US federal level data privacy legislation. Moreover, while the Brussels Effect certainly applies in these cases, the highly consultative relationship between EU officials and their American interlocutors in both private and public sectors also reflects interactions described by the NIA.

Meanwhile, the EU and US engaged in two years of negotiations to develop a new solution to data transfers that would satisfy the requirements of the European Court of Justice (ECJ) in a pattern that is consistent with what the New Interdependence Approach would predict. The new agreement, announced in March 2022, appears to be one in which the US has made significant concessions to EU requirements. While the final legal text has yet to be released, lead negotiators from the EU and US have stated that they went through each line of the ECJ ruling to determine what mechanisms could be put in place to ensure that the agreement would be robust to future legal challenges.[49] This involved threading a needle to accommodate the very different legal philosophies of the two regions.

In a final development, the U.S. Congress in June 2022 announced a bipartisan, bicameral draft comprehensive bill, the American Data Privacy and Protection Act. This bill has many features of the GDPR. Thus, the US case study elaborates on the ideational shift the United States has made since it first negotiated the Safe Harbor agreement in 2000 and considers

[48] 2020, "Apple Policy Statement: Our Commitment to Human Rights." https://s2.q4cdn.com/470004039/files/doc_downloads/gov_docs/2020/Apple-Human-Rights-Policy.pdf.
[49] One academic went to so far as to say that US regulators might as well have negotiated with the ECJ. Statement not for attribution, EU-US TTC Working Group Roundtable, March 2022.

concessions it ultimately made as the data governance story unfolded. The research also demonstrates how the European Court of Justice has imposed on EU foreign policy.

Japan is the third case study. Prime Minister Shinzo Abe articulated a broader grand strategy for transforming Japan into a "normal" international actor that would claim a more pronounced global leadership role for itself. His grand strategy included shoring up the global trading system and preserving what he dubbed a "Free and Open Indopacific" to counterbalance Chinese ambitions in the South China Sea. Abe saw the EU as a vital partner in this mission and made a priority of folding relations with the European Union into mainstream Japanese diplomacy. Data flows formed a key piece of the greater geostrategic puzzle.

The Japan case sketches out the geopolitical context surrounding its adoption of European data privacy conventions and shows how strategic imperatives created an aperture for the EU to bring Japan closer to its data privacy preferences. While the EU and Japan had enjoyed a long-standing and friendly dialogue since the end of the Cold War, their relationship had always been subordinated to relations with the United States and China. China's increasingly aggressive foreign policy toward Japan, coupled with the US's withdrawal from the Trans-Pacific Partnership (TPP) and its general retreat from leadership in multilateral fora, raised the salience for both the EU and Japan to cooperate on trade and data flows. While these developments changed the environment around the EU and Japan, Abe provided the decisive leadership that could leverage the relationship of trust between the two sides to conclude a troika of agreements that have transformed the EU-Japan relationship. Since then, their coordination through the *Data Free Flows with Trust* initiative has helped advance the global discussion of

instruments and rules to facilitate cross-border data transfers. In addition, their interactions now show evidence of interactions that are predicted by the NIA.

Chapter VII provides concluding comments that summarize the findings of this research and outline thoughts for the future.

1.8 Limits of Research

Because they focus on large economies, this limits the insight the research can yield regarding smaller nations. One would expect, for example, that smaller countries who benefit from global trade would prefer the US or European model, though they will have to consider China as part of their political calculus. Singapore is a country that has adopted data privacy regulations described as taking a middle ground between the US and European system but appears to be moving in the direction of more European-style data governance regulation.[50] Bahrain is another small country that has adopted more GDPR-like regulations and would, as another authoritarian regime, invite a useful comparison to China.[51] An additional constraint is that this research includes only one major authoritarian regime, China. China is an atypical authoritarian power because of: 1) its status as the second largest ecnomy, which generates idiosyncratic scale advantages not available to smaller authoritarian nations, and 2) its characteristic of responding quite actively to popular demands, as has been documented by authors, including Diana Fu, Bruce Dickson, and Edward Cunningham et al.[52] China's responsiveness to

[50] For a comparative review of data privacy and protection laws in Asia, cf. Robert Walters, Leon Trakman, and Bruno Zeller, *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches* (Springer, 2019).
[51] *Data Protection Laws of the World*, (2021).
[52] Diana Fu, *Mobilizing without the Masses: Control and Contention in China*, Cambridge Studies in Contentious Politics, (Cambridge: Cambridge University Press, 2017). https://www.cambridge.org/core/books/mobilizing-

citizen demands is similarly borne out in the data privacy case study. In this sense, the research does not consider China as a representative authoritarian regime. It will be useful for future research to look in greater detail at countries like Saudia Arabia to compare how they govern data.

A third observation is that this research largely articulates data privacy issues and focuses less on data protection. Europeans often refer to these terms interchangeably for practical purposes, as noted in Appendix 1. However, the distinction is important for practitioners. The focus on data privacy rather than data protection is entirely practical but does not suggest that data protection is not equally important. Data protection bleeds quickly into cybersecurity and would thus stray from the core theoretical framework of this effort.

A fourth limitation of this research is that it fails to include enough of a developing world perspective.[53] One important reason is that developing country scholars have yet to focus on data protection as a research topic in their country. China has tried to present itself as the voice of developing countries and increasingly enlists their support at the International Telecommunications Union (ITU) to change the rules on data flows. Specifically, they seek to reframe data governance as a multilateral rather than a multistakeholder question. A multilateral framework would remove civil society from the data governance debate and shift it to a top-down, state-driven dialogue. This is anti-democratic from the Western perspective. China's

without-the-masses/FE8DA14FD770D0FACF35E9979A3BB8DA. Bruce Dickson, *The Party and the People: Chinese Politics in the 21st Century* (Princeton: Princeton University Press, 2021); Edward Cunningham, Tony Saich, and Jesse Turiel, *Understanding CCP Resilience: Surveying Chinese Public Opinion Through Time*, Harvard Kennedy School Ash Center (2020).

[53] Cf.UNCTAD, *Digital Economy Report 2021: Cross Border Data Flows and Development*., pg.

relatively successful move to dominate the discussion as a self-appointed representative of the developing world skews our view of Global South data governance preferences.[54]

A final challenge to this research is that the data protection landscape is rapidly changing. Data governance has only recently climbed to the top of the agenda for democratic governments. As such, they are still playing catch-up to understand how China, Russia, and other authoritarian nations have used misinformation and disinformation to tilt the geopolitical playing field in their favor. Whereas previously, the US attitude toward maximizing data flows in the interest of promoting global trade has prevailed, rising cyberattacks and the trade war with China have exposed US vulnerabilities that are prompting a fundamental reevaluation of this stance.[55] As importantly, there are disagreements among Western democratic nations on approaching data flows. This has created fissures and impediments to developing a consensus.

1.9 Conclusion

The broad conclusion from the research is that the GDPR has generated significant changes in the data governance regimes of the three countries studied. While all the countries studied have signed up to the UN Declaration on Human Rights and frequently access the human rights narrative in a policy context, none of them has explicitly integrated the European human rights approach into their data privacy legislation. The geopolitical implications continue to play out as the rivalry between liberal democratic and authoritarian unfurls. Developing

[54] James Griffiths, *Great Firewall of China* (Bloomsbury Publishing, 2019). See especially Chapter 20, "The Censor at the UN: China's undermining of global internet freedoms."
[55] Henry Farrell and Bruce Schneier, "Common Knowledge Attacks on Democracy," *Research Publication No. 2018-7* (2018).

countries looking for models to protect or reform domestic institutions that interface with private data will be caught in the cross-fire among the competitors.

2 Chapter II: GDPR in the EU & Global Context

This chapter provides the descriptive background to the EU's strategy for the digital age, for which the GDPR and the Free Flow of Data (FFoD) regulation collectively serve as the foundation.[56] While the GDPR came first in a string of new regulations, it was preceded by the recognition that the explosion of cross-border data flows and the market impact of globalization required a more comprehensive response. Understanding this context helps explain why the EU defends and seeks to extend the adoption of the basic principles of the GDPR throughout the world. Moreover, in many cases, the GDPR forms the legal basis for which other European Commission (EC) regulations are put forward, such as the recent Digital Services Act (DSA) and the Digital Markets Act (DMA), discussed below.[57] This chapter explains some of the history that led to the GDPR and shows how it differs from its predecessor, the 1995 Data Protection Directive (DPD). Finally, it puts the GDPR in a global context, showing from a 50,000-foot view how China, the EU, and the US approach to data privacy and data governance writ large are different. This chapter is foundational to understanding the case studies that follow.

2.1 Background to the EU Strategy for the Digital Age

The "human-centric" emphasis of the *Strategy for the Digital Age* defines the EU's democratic project, its legislative agenda, and to a significant degree, its interactions with nations

[56] While the GDPR covers personally identifiable data and attempts to restrict data flows that threaten privacy, the FFoD covers non-personal data and largely ensures the free flow of data across international borders. Cf. IAPP, "EU's Strategy for Data: What the DSA, DMA, DGA mean for privacy," (December 12, 2021 2021).

[57] The European Commission is the body that puts forward new regulations for the EU. These assume legal force when voted upon by the European Parliament and the Council of the European Union. The latter is not to be confused with the Council of Europe, which is a non-EU body tasked with promoting human rights.

beyond the EU.[58] The EU's digital strategy is intended to ensure the benefits of global openness while concurrently defending its *Charter of Human Rights*. This differentiates the EU from its transatlantic partner, the US, and other English-speaking liberal democracies that rhetorically emphasize the free flow of commerce over protecting individual rights in the commercial context. Not surprisingly, the digital strategy also sharply differentiates it from China. It is easy for the casual observer to underestimate the degree to which EU officials recite the importance of the *Charter* as they engage in their Working Group and parliamentary debates. The European Commission's 2017 report to the European Parliament on global data exchanges and personal data protection provides a classic example of a long-standing framing that connects individual protection to a vibrant market economy:

> "Respecting privacy is a condition for stable, secure, and competitive global commercial flows. Privacy is not a commodity to be traded. The internet and digitization of goods and services has transformed the global economy and the transfer of data, including personal data, across borders is part of the daily operations of European companies of all sizes, across all sectors. As commercial exchanges rely increasingly on personal data flows, the privacy and security of such data has become a central factor of consumer trust…. In the digital era, promoting high standards of data protection and facilitating international trade must thus necessarily go hand in hand."[59]

The economic linkage with fundamental rights began initially on paper and became integral to policymaking over time. This linkage occurred as civil society, think tanks, NGOs, and corporate entities increasingly engaged with parliamentarians and lawmakers. The latter engaged with the outside world, establishing a panoply of new rules, norms, guidelines, and "soft laws"

[58] A European strategy for data, (European Commission, 2020).
[59] Exchanging and Protecting Personal Data in a Globalised World, (Brussels: European Commission 2017).

and responding to the global environment.[60] While in the 1990s, data regulation in the EU was linked to the integration of the Single Market, by the 2010s, officials gradually perceived the regulation of its digital markets as a defensive measure inextricably linked to industrial policy. This narrative was initially directed at the US, whose firms had come to dominate the European business landscape, but today it is increasingly pointed at China and Russia. A core outcome of this development is that the EU's *Charter on Fundamental Rights* now imposes constraints on its foreign policy—particularly through legal interpretations by the European Court of Justice (ECJ).

From an internal perspective, the EU has a comparative advantage in regulation.[61] The EU's self-perception and confidence have grown as it has witnessed the global diffusion of its regulation. However, the EU also sees itself as vulnerable from multiple angles. The obvious vulnerability from US shores is Europe's reliance on NATO and the United States for its military security umbrella. This perception of weakness was heightened by the Obama administration's pivot to Asia[62] and exacerbated by the Trump administration's threat to withdraw from NATO altogether.

The less obvious vulnerability to many American observers is the degree to which Europeans perceive the US's digital dominance on the continent as "increasingly becoming

[60] The term "soft law" refers to quasi-legal instruments (like recommendations or guidelines) which do not have any legally binding force, or whose binding force is somewhat weaker than the binding force of traditional law.
[61] For literature on the rise of the regulatory state in general, cf. Giandomenico Majone, "The Rise of the Regulatory State in Europe," in *West European Politics*, ed. Wolfgang C. Muller and Vincent Wright (1994). See also David Bach and Abraham L. Newman, "The European regulatory state and global public policy: micro-institutions, macro-influence," Article, *Journal of European Public Policy* 14, no. 6 (09/01 / 2007).
[62] Lius Simon, "Europe, the rise of Asia and the future of the transatlantic relationship," *International Affairs* 91, no. 5 (September 2015 2015), https://doi.org/https://doi.org/10.1111/1468-2346.12393.

synonymous with economic dominance... such dominance comes with the power to infringe on the sovereignty of others," as Emily Wu suggests.[63] As a result, Europeans often feel that they are becoming or already are a "digital colony" of the US's big tech firms.[64] Calls for digital sovereignty, however loosely defined, have become a popular cry in many European capitals. Indeed, Theodore Christakis argues that it is through regulation of the digital space that the EU exercises its sovereignty in resistance to the US digital juggernaut.[65] In this sense, Europeans view their strong regulations as a defensive tactic rather than an explicitly protectionist move. Protectionism is a charge leveled by US actors against the EU with some frequency.

Europe has been largely absent from the creation of firms that are large-scale innovators with significant market share in the digital economy. As the Economist points out, "Europe is both gnome and giant in the tech world. The continent has lots of cutting-edge technology but hardly any significant digital platforms. It accounts for less than 4% of the market capitalization of the world's 70 largest platforms (America boasts 73% and China 18%). At the same time, the EU is a huge market, with a population of more than 500m, which no tech titan can ignore. It contributes about a quarter of the revenues of Facebook and Google."[66] When the ICT revolution initially took off in the late 1990s, Alcatel of France, Ericsson of Sweden, and Nokia of

[63] Emily Wu, *Sovereignty and Data Localization*, Harvard University Belfer Center for Science and International Affairs (Cambridge, 2020).
[64] Cf. for example, Julien Nocetti, " Is Europe a "digital colony" of the United States?," *Politique étrangère* vol. , no. 3, , pp. (2021), https://doi.org/ https://doi.org/10.3917/pe.213.0051 See also Carla Torres, ed., *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry-European Council on Foreign Relations* (ECFR, 2020). Note that the Europeans are not the only country who complain about the dominance of American firms in the digital space. India is also a vocal plaintiff in the case against the biggest cloud service providers in its country, Amazon Web Services, Google, and Microsoft.
[65] Theodore. Christakis, *"European Digital Sovereignty"*, Data Institute University Grenoble Alpes (December 2020). Pg. 10.
[66] "The EU wants to set the rules for the world of technology," *The Economist*, February 20, 2020.

Finland were major telecoms players whose global market share rocketed to the top. However, as much as Europe's firms benefitted from globalization, by the mid-2010s, they lost key competitiveness in hardware, including ICT equipment and semiconductors. Until 2012, Nokia was a world leader in smartphone manufacturing. Its revenues peaked in 2008, after which it rapidly lost market share to Apple and Samsung and finally sold its phone business to Microsoft in 2013.[67] Europe today holds 15% of the global market share in ICT revenues compared to the US's 35% and China's 11%--a shrinking share since 2010. As critically, Europe never developed truly global leading-edge software or social media. European firms played no role when Google and Facebook emerged in the late 1990s and 2000s. There are no European internet-based platforms of the scope and scale enjoyed by US and Chinese firms. At this stage, the returns to scale on the large digital platforms are such that Europe has little chance of catching up with the virtual monopoly status that American firms occupy on the continent. Many pundits argue, they are too far behind the innovation curve.

2.2 European policy entrepreneurship in historical context

While European industry was slow to innovate, government bodies were not. They quickly recognized the importance of managing the downstream effects of data aggregation and engaged in policy entrepreneurship. The current digital strategy is built on decades of experience in championing privacy and data protection issues, arguing that they are central to the economic well-being of the Union.

[67] Data according to Statista.com. Currently Nokia focuses exclusively on data networking services and telecom equipment, competing head-to-head with China's Huawei.

When the EU finally passed the DPD, the discussion and debate had been ongoing for 15 years. The "Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (Data Protection Directive 95/46/EC) was established to provide a regulatory framework to guarantee the secure and free movement of personal data across the national borders of the EU member countries, in addition to setting a baseline of security around personal information wherever it is stored, transmitted or processed. The directive took effect in 1998.[68]

The DPD was relatively early in the life of the newly formed European Union, which came into existence in its current form with the Maastricht Treaty of 1992. As with today's ongoing contest over a European banking union, there was considerable resistance to data privacy standards in the 1970s. Over time, advocates argued for a move toward a centralized, supranational solution to the quandaries raised by having differing (or non-existent) data privacy regulations in the disparate member nations. The European Parliament originally recommended pan-European data privacy rules, but the Commission rejected these suggestions, arguing that supranational policies would raise the cost of doing business in the EU.[69] Meanwhile, the Council of Europe, an intergovernmental body founded to advance human rights, jumped ahead of the Commission when it passed *the Convention for the Protection of Individuals with Regarding Automatic Processing of Personal Data* in 1981. Yet, in a sign of how weak the institutional

[68] "EU Data Protection Directive," Electronic Privacy Information Center (EPIC), accessed October 1, 2021, https://archive.epic.org/privacy/intl/eu_data_protection_directive.html. This general Data Protection Directive has been complemented by other legal instruments, such as the e-Privacy Directive for the communications sector. There are also specific rules for the protection of personal data in police and judicial cooperation in criminal matters, e.g. the Framework Decision 2008/977/JHA.
[69] Newman, *Protectors of Privacy*., pp. 83.

capacity for implementation was, only four of the nine ratifying member nations ever took national action to implement domestic legislation supporting the convention.

In the 1980s, the data privacy community "underwent a transformation from a policy network comprising primarily legal experts to an institutionalized group of substate actors with domestic authority," according to Abraham Newman's account.[70] Picking up where the European Parliament left off when it initially failed to garner European Commission support for privacy regulation, Newman posits that a network of trans-governmental actors were the primary driver of data privacy regulation at the supranational level. They were an early example of policy entrepreneurship often discussed in the context of EU financial market integration. Because of their technical expertise, transgovernmental actors could define problem areas and suggest policy solutions. As with financial services regulation for market integration, the EU governing bodies lacked the budget to rely on in-house technical experts. Transgovernmental actors filled the budget gap by contributing their knowledge of policy subsystems and advice on formulating language in the data directive. They later played an active role in rule development and enforcement.[71]

Most importantly, data privacy experts were able to frame the need for regulation in the context of the Single European Market integration. In doing so, they convincingly articulated the fear that mobile capital within Europe would move to countries with more lax data privacy legal requirements. They argued that if data could flow freely across borders without

[70] Newman, *Protectors of Privacy*., pp. 83.
[71] *ibid*, pp. 79.

harmonized standards, it would undermine the enforcement powers of national data regulators. This provided the momentum to get the directive passed.

The 1995 DPD benefited from the historical contingency of being promulgated just ahead of the unanticipated explosion of the internet and the progressive digitization of the global economy. Its focus was largely internal, and as a result, the dialogue around data privacy happened largely outside of the Transatlantic relationship. Had the United States already established its dominance in the digital economy, we might have seen a different outcome for data flow regulation in Europe. As a result, there is a stark contrast between the relative convergence of US/EU finance and banking regulation on the one hand and regulatory divergence on data privacy on the other.

Today, Transatlantic attitudes toward data privacy are contested on various levels, one of which is structural. While the EU has pursued a comprehensive approach to data privacy since the 1990s, the United States has consistently pursued a limited approach. Historically, the United States has pursued a fragmented regulatory environment that favored corporate control and data ownership with fewer firm obligations to the consumer regarding notice and consent. While the United States has exceptions in the form of education and health industry-related data privacy rules (under the FERPA and HIPAA laws), regulations do not cover online retail services or social media.

By contrast, as argued by Posner and others, considerable Transatlantic debate and compromise fostered regulatory convergence on financial services and extensive integration

between the US and the EU.[72] So while in financial services, the EU and US actively cooperated on regulation, data privacy regulation largely flew under the radar screen of Transatlantic relations. It was, therefore, not subject to the strong influence of American thinking, which by the 1990s diverged considerably from that of the EU. In sharp contrast, the Clinton administration (1993-2001) eschewed strong data flow regulation. Instead, the administration was committed to maximizing data sharing on the premise that unencumbered digital traffic would foster innovation and economic productivity growth.[73] In a way, this was not surprising given the near euphoria that existed in the late 1990s when "electronic mail," or email, and the Internet first found their way into everyday life.

In sum, the EU's policy entrepreneurship developed a culture of data privacy protection over several decades that has since become embedded practice in EU institutions. The clear divergence from the US approach, shown in Chapter VI, laid the foundation for the EU to be a leader in data governance when the Cambrian explosion of digitization occurred.

2.3 The DPD to the GDPR

In 2012, the EU proposed a revision to the 1995 DPD to tackle the rapid digitization of the global economy. This proposal later became the GDPR. The scope and scale were initially limited to a pragmatic focus on economic exchange and trade flows.[74] The catalytic event that spurred the EU and many other nations to consider more strategic reform was the 2013 Edward

[72] Posner, "Making Rule for Global Finance: Transatlantic Regulatory Cooperation at the Turn of the Millennium." See also Abraham Newman and David Bach, "The European Union as hardening agent: soft law and the diffusion of global financial regulation," Article, *Journal of European Public Policy* 21, no. 3 (01/01 / 2014).
[73] Henry Farrell and Abraham Newman, *Of Privacy and Power* (Princeton and Oxford: Princeton University Press, 2019). Pg. 130.
[74] Napoleon Xanthoulis, *Negotiating the EU Data Protection Reform: Reflections on the Household Exemption*, vol. 441 (2013).

Snowden revelations. Snowden was a former national security contractor with access to top-secret documents. He disclosed information about many US government surveillance programs, including those managed by the National Security Agency (NSA).[75] The documents he released uncovered the extent to which the US government leveraged public platforms to surveil social media and foreign nationals. Worse still, they also encroached on private foreign telecommunications; and, confirmed what others, notably Caspar Bowden, had already flagged. Bowden was a cofounder of the Foundation for Information Policy Research and a privacy advisor to Microsoft. Between 2011 and 2013, he made a series of speeches highlighting how US laws allowed for mass surveillance of foreign citizens in direct contradiction to the *Charter of Fundamental Rights*. To his regret, his arguments received scant attention within the EU; he was often openly mocked in the United States.

The Snowden revelations struck like a lightning bolt into the heart of Europe, stirring waves of social activism to secure better citizens' protection from corporate and government monitoring. As argued by Rossi and others, Snowden's global surveillance revelations inverted the direction of the European Parliament's debate on the GDPR. Before Snowden's leaks, corporations were predominantly shaping Europe's privacy rules. [76] After the disturbing revelations, communications and internet privacy issues became paramount across the EU and thereby blunted the power of corporations to influence the policy outcome. In Germany, for example, there had been a long tug-of-war between privacy activists and companies. On the one

[75] EWEN MACASKILL and GABRIEL DANCE, "NSA Files: Decoded," *The Guardian*, November 1, 2013, https://www.theguardian.com/us-news/the-nsa-files.
[76] Agustín Rossi, "How the Snowden Revelations Saved the EU General Data Protection Regulation," *The International Spectator* 53, no. 4 (2018/10/02 2018), https://doi.org/10.1080/03932729.2018.1532705, https://doi.org/10.1080/03932729.2018.1532705.

hand, activists had lobbied for better protections, successfully resisting Google's aggressive street mapping of German and Austrian cities in one major instance.[77] On the other hand, German corporations and even *Länder* vocally argued to water down the most stringent features of the GDPR. Snowden handed the German activists a particularly powerful weapon with the disclosure that the US's NSA had actively monitored German Chancellor Angela Merkel's cell phone. As Farrell and Newman note, "the leaks revealed important connections between commercial data transfers and government surveillance….Privacy advocates used this irrefutable evidence to gain access to opportunity structures that had previously been closed off so that they could try to insulate European privacy rules from transnational pressures."[78]

While the US's massive data sweep had targeted many nations, the supranational EU was uniquely positioned to respond rapidly and comprehensively to the NSA surveillance controversy. It had created the institutions with subject area expertise, capacity, and experience gained from negotiating and passing the DPD. The Snowden revelations erupted into a whirlwind of regulatory activity that resulted in the passage of the GDPR and generated a strategic agenda more far-reaching than had previously been contemplated. The next section discusses how the GDPR built on the DPD for the 21st century digital economy.

2.3.1 The new personal data protection regime

The GDPR is both the product of its predecessors and a radical change from what came before. It incorporated elements of the DPD, originating from the OECD's *Guidelines Governing*

[77] https://bigthink.com/strange-maps/germany-street-view/
[78] Farrell and Newman, *Of Privacy and Power*. Pg. 125.

the Protection of Privacy and Trans-Border Flows of Personal Data. In 1980, the OECD created the following seven principles:[79]

- Notice – individuals should be notified when their personal data is collected.
- Purpose – use of personal data should be limited to the purpose for which it was collected.
- Consent – individual consent required before personal data is shared with other parties.
- Security – collected data should be secured against abuse or compromise.
- Disclosure – data collectors should inform individuals when their personal data is being collected.
- Access – individuals should have the ability to access their personal data and correct any inaccuracies.
- Accountability – individuals should have a means to hold data collectors accountable to the previous six principles.

All seven of these guidelines carried over into the DPD and the GDPR.

The DPD and the GDPR both conceptualized data privacy and protection as a human right. As human rights, they impose on EU member states the obligation to constrain government abuse and ensure a more level playing field between public authorities, corporations, and individuals—even if the purpose of data processing, for example, is being done for the benefit of the individual.[80] The human rights principle is the *Leitmotiv* that unifies the structure of both regulations over time. However, between the 1995 DPD and the 2016 GDPR, the EU passed the 2012 *Charter of Fundamental Rights,* which gave the data protection mandate more legal teeth. Privacy and data protection were enshrined in the EU Treaties and in the 2012 *EU Charter of Fundamental Rights* articles 7 and 8.[81] Thus, the Charter could be used in court matters as a

[79] Nate Lord, "What is the Data Protection Directive," *Digital Guardian's Blog*, September 12, 2018, https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.
[80] Kuner, "An international legal framework for data protection: Issues and prospects."
[81] "Data Protection," European Data Protection Supervisor, accessed September 24, 2021, https://edps.europa.eu/data-protection/data-protection_en. In fact, the GDPR establishes 8 new individual rights.

legal precedent in enforcement cases.[82] The *Charter* explicitly addresses privacy and data protection issues as follows:[83]

> *Article 7 : Respect for private and family* life
> Everyone has the right to respect for his or her private and family life, home and communications.
> *Article 8 : Protection of personal data*
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

The legal power implied by the *Charter* incentivized a more robust data protection framework. How was this achieved, and what made the GDPR different from its predecessors? First, the GDPR is a regulation, whereas the DPD is a directive which carries important consequences. An EU directive is a legal act that requires member states to accomplish a particular set of goals without dictating the means to do it. The Commission outlines certain rules which must be met, but each member state decides how to ensure compliance through national laws. Member countries may enact (or transpose) appropriate legislation by a specified date, normally two years.

Regulations are binding legislative acts applicable to every member state and can be immediately enforced through law like any local legislation. Regulations supersede local legislation unless the local one is stricter than the EU regulation. Germany, for example, has stricter

[82] Svetlana Yakovleva, "Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade 'Deals'?," *World Trade Review* 17, no. 3 (2018).
[83] European Union, "Charter of Fundamental Rights of the European Union."

data protection regulations than the EU. Regulations are more prescriptive, inflexible pieces of legislation. No local level deliberations are allowed regarding the implementation of EU regulations as they are with directives. Regulations take effect upon ratification by the EU parliament. In their legislative power, regulations are unparalleled to any other constituent of EU law.[84]

Second, the GDPR significantly deepened individual protections. It changed the balance of power between corporations as data processors and consumers, generally referred to as "data subjects," in favor of consumers. From mere data subjects, they were also promoted to data controllers because they now have greater agency over who can gather and hold their data. It did so chiefly by tightening consent rules for the digital era and by adding two new rights: the right to be forgotten and the right to data portability. Thus, some have referred to the GDPR as a "Copernican revolution"[85] in data protection. The Commission's own words summarize the intent of the regulation in their 2017 communication to the European Parliament and the Council, "Exchanging and Protecting Personal Data in a Globalised (sic) World":

> "The reform of EU data protection legislation adopted in April 2016 puts in place a system that both ensures a strong level of protection and is open to the opportunities of the global information society. In giving individuals more control over their personal data, the reform strengthens *consumer trust* in the digital economy."[86]

Consumer trust in the digital economy was seen in Europe as a key driver for growth and was thus central to adopting the additional rights to data portability and the right to be forgotten. Trust, in fact, also served as a piece of the rationale for the other revolutionary update to the DPD: the GDPR vastly increased the scope of its extraterritoriality clauses. The expansion

[84] https://ec.europa.eu/info/law/law-making-process/types-eu-law_en
[85] Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," (02/06 2012).
[86] Exchanging and Protecting Personal Data in a Globalised World, Short.

of this clause has generated a tectonic shift in corporate and national behavior. The framing of consumer trust as a cornerstone of economic vitality also spawned Japan's data governance initiative, The Osaka Track, in 2019 under the moniker "Data Free Flow with Trust."[87] This drive continues today in working groups at the OECD and is focused particularly on the thorny issue of government access to private sector data. Thus, there were two GDPR impact trajectories: one toward the individual consumer and another toward the firm or country. The section below provides a discussion of some of the specific changes. The case studies will show how nations, US states, and companies responded to these changes.

2.3.2 Territorial Scope

From a geopolitical perspective, expanding territorial scope beyond that of the DPD is the most important. As a result of the change, firms offering services to individuals residing in the EU are subject to the GDPR even if they are not domiciled there or do not have a physical presence there.[88] This had little impact from the perspective of EU firms since they were already in compliance. However, from the third country's perspective, the impact has been significant in many cases. For example, financial services firms offering products within the EU that had not previously been subject to DPD requirements would have to introduce new compliance layers onto their operations. Any institution providing financial services to an EU resident, e.g., PayPal, was subsequently required to follow the GDPR in its entirety. As such, the GDPR materially broadens the number of firms subject to EU regulation than under the DPD.

[87] Masumi Koizumi, "Japan's pitch for free data flows 'with trust' faces uphill battle at G20 amid 'splinternet' fears," *Japan Times* (June 27, 2019).
[88] https:/ /gdpr.eu/what-is-gdpr/

Some firms doing business with the EU needed to decide whether they would shift toward keeping the data they collected within the EU rather than holding it in the cloud overseas. The advantage of keeping it overseas was operational efficiency and data aggregation that could yield market insight. Alternatively, firms could roll out GDPR standards across their global operations to comply with the new regulation. Scholarly articles have questioned whether data localization would be the *de facto* result. Indeed, data localization has been a rising trend around the globe that many attribute to the GDPR. There is evidence to support this argument. Microsoft, for example, announced in 2021 that it would create the capacity for customers to determine if they would keep their EU data held through Microsoft's cloud services exclusively on EU-based servers.[89] However, the trend toward data localization in its many forms was already observed prior to 2016. Sometimes captured under the term "data nationalism," this trend has continued to gain momentum in certain parts of the world.[90] The trend is particularly pronounced among non-democratic nations seeking to surveil their populations for the purpose of social control.

2.3.3 Definition of Personal Data

One of the most important changes from the DPD to in the GDPR is the definition of personal data. The GDPR's definition reflects changes in technology and how organizations collect data about individuals since 1995. Profiling or developing a snapshot of an individual's preferences using browser history and purchase history is no longer permissible under the GDPR

[89] Brad Smith, "Answering Europe's Call: Storing and Processing EU Data in the EU," *Micosoft EU Policy Blog*, May 6, 2021, https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/.
[90] Anupam Chander and Uyen P. Le, "Data Nationalism " *Emory Law Journal* 64, No. 3 (2015), https://ssrn.com/abstract=2577947

without explicit consumer consent. Under the DPD, personal data is defined as names, photos, email addresses, phone numbers, addresses, and personal identification numbers (e.g., social security, bank account). However, it did not address what in 1995 was a relatively limited practice of consumer profiling. Under the GDPR, personal data is more broadly defined as any information that could be used, on its own or in conjunction with other data, to identify an individual. This data includes IP addresses, mobile device identifiers, geolocation, and biometric data (e.g., fingerprints, retina scans). The GDPR also covers data related to an individual's physical, psychological, genetic, mental, economic, cultural, or social identity. The GDPR thus updates and expands the conception of personal data to reflect features of the digitized economy not yet prevalent in 1995. It also reflects the human rights mandate of the *Charter of Fundamental Rights*.

2.3.4 Data Inventory & Privacy by Design

Another key change in the GDPR is that organizations must actively track how and where data is stored and used throughout the supply chain. To do so, they must adopt risk management tools and build security and privacy into their operations from the inception of systems and processes—that is, they must implement "privacy by design." Firms shall consider the privacy of collected data at all steps in developing business concepts and that data settings default to the most restrictive data collection practices, assuming that individuals would prefer less rather than more information collected about them. Privacy by design also requires controllers to discard personal data when they are no longer using it so that it cannot be reused in

infinite ways. Infinite reuse of data has been widely discussed in a great deal of academic literature as a potential source of abuse.[91]

2.3.5 Penalties

A final key change is the enhanced independence and power of Data Protection Authorities (DPAs), enabling them to impose fines on corporations of up to two percent of their global income. As the EU's GDPR website notes, "The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher…. The more serious infringements go against the very principles of the right to privacy that are at the heart of the GDPR; i.e., the right to be unobserved and the right to be forgotten. These infringements could result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher."[92] Since the passage of the GDPR, the largest fine that the EU has doled out was by Luxembourg, which fined Amazon €746 mn ($887mn) for violations relating to its business practices around data breaches.[93] According to DLA Piper's most recent survey of GDPR enforcement, EU member nations have increased their fines sevenfold in 2021 compared to the previous year. No firm has ever been fined the amount allowed under the provisions for violating the principle of the right to privacy.[94]

[91] See for example Lizhi Liu, "The Rise of Data Politics: Digital China and the World," *Studies in Comparative International Development* 56, no. 1 (2021/03/01 2021), https://doi.org/10.1007/s12116-021-09319-8. See also Kuner, "An international legal framework for data protection: Issues and prospects."
[92] "What are the GDPR Fines?," GDPR.EU, accessed September 25, 2021, https://gdpr.eu/fines/.
[93] Sam L. Shead, "Amazon hit with $887 million fine by European privacy watchdog," (July 30, 2021). https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html.
[94] DLA Piper, *GDPR fines and data breach survey: January 2022* (2022).

2.3.6 New Rights

As mentioned, the GDPR also granted individuals new rights. The most well-known of these is the right to be forgotten, which became a cause célèbre in 2014 when the European Court of Justice ruled in favor of a Spanish man who sued Google to have personal data removed from Google internet search engine results.[95] Although not an absolute right, it allows individuals to expunge certain information from the public record that could damage their social reputation. In the Spanish case, a man sought to expunge information regarding the forced sale of his property that had since been resolved.

The other critical right gained for individuals is the right to portability, allowing consumers to move their personal data from one vendor to another. This has played an important role in promoting market competition, albeit as part of a much larger regulatory agenda. The banking sector is a key example. EU regulators had already taken on the monumental task of responding to the Global Financial Crisis (GFC) with measures intended to improve private sector data sharing with the European bank regulators and the European Central Bank. When the GDPR passed in 2016, financial services had to contend with consumer requests to have their data deleted or ported to other banking institutions. The extraterritorial extension of the GDPR meant that it was not only European bankers who were affected by the changes but also global platforms like Citibank, JP Morgan, and others. For a discussion of the significance of the GDPR in the financial services context, see Appendix 2.

[95] "How a Spanish man took on Google over privacy concerns and won," Euronews updated January 27, 2017, https://www.euronews.com/my-europe/2017/01/27/how-a-spanish-man-took-on-google-over-privacy-concerns-and-won.

The two new rights imply significant data management-related externalities for firms. In order to respond to consumer requests to have their data removed, corrected, or ported required that the firms investigate much more rigorously what data they held and where it was held. Many firms, especially platform-sized firms with many business units, never coordinated their data gathering efforts. An illustrative example is a 2022 article on Facebook describing an internal report showing executives do not comprehensively understand where their data flows.[96] The second-order effect of the data inventory requirements was that firms became more aware of their sources of vulnerability to data breaches. Once the vulnerabilities have been identified, firms and countries are in a far better position to mitigate them. Moreover, because the GDPR raised the standards for informing consumers and regulators about data breaches, there was a meaningful incentive to have an accurate understanding of the inventory.

2.4 Digital Privacy Ecosystem

The example in Appendix 2 shows how the GDPR interfaced with financial regulation to achieve better oversight of data flows and increased market competition. These occurred as part of an EU response to the GFC. However, this effort extended beyond financial services to the wider economy with the EU's strategy for the digital age. As with the financial services industry, the EU built on the foundation of the GDPR to address data governance writ large and market competition issues. Thus, it spawned an array of proposed regulations meant to

[96] Lorenzo-Franceschi Bicchierai, "Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document," *Motherboard*, *Vice*, April 26, 2022, https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

construct the infrastructure for a trust-based digital economy. Around the same time, some Europeans voiced the need for "digital sovereignty." The definition of digital sovereignty has been the focus of enormous debate, starting with how to define digital, data, and sovereignty separately in this context. The simple question, "Who is the sovereign?" points to the complexity of the matter. One EU Parliament paper defines digital sovereignty as "Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)."[97] This definition sounds like a protectionist note that contradicts the Commission statements several years prior. [98] The EU has continued to promote open trade flows, and digital policy is an integral part of its strategy.

The 2021 release of the European Commission's ambitious "2030 Digital Compass: the European way for the Digital Decade"[99] articulated a new direction not so much toward digital sovereignty, but toward reduced vulnerability to outside influence. The document reflects the EU's internal sense of fragility in three regards. First, they felt trapped in an unhealthy trade war between the United States and China, in which the Trump administration sought to coerce and bully European actors into doing its bidding, largely through the security threat of withdrawing from NATO. Second, because the EU has little of its own internal semiconductor design, manufacturing, and assembly capacity, it was especially vulnerable to global supply chain

[97] Christakis, *"European Digital Sovereignty"*. See also Tambiama Madiega, "Digital Sovereignty for Europe," *EPRS Ideas Paper* (July 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf; Madiega, "Digital Sovereignty for Europe."

[98] The EU's conception of digital sovereignty is not to be confused with China's quest for cybersovereignty, which explicitly censors the internet and seeks to exclude foreign influences. China's cybersovereignty includes requirements for data localization that the EU does not promote.

[99] 2030 Digital Compass: the European way for the Digital Decade, (Brussels: European Commission, 2021).

risks in both the United States and China.[100] Finally, Europe was vulnerable to Russian disinformation campaigns that influenced local EU elections and swayed the Brexit vote against the broad continental consensus in favor of the UK remaining within the EU.[101] The Commission's response to this three-front vulnerability was a comprehensive digital and cybersecurity strategy articulated in a series of documents that included the *Digital Compass* just mentioned as well as the *Cybersecurity Strategy (2020)*, the *Proposal for Regulation on AI (2021)*, and the *Coordinated Plan for AI (2021)*. In these documents, the European Commission actively reinforced its human rights and dignitary approach to business and government and set itself apart from the United States and China. These documents primarily addressed the issues of the EU physical infrastructure to support the internet and cyberspace and set a strategy to continue promoting a global and open internet.

European Commission officials have built a digital governance structure based on these documents. Throughout 2021, the Commission released a host of draft legislation to undergird the digital decade to cultivate a healthy digital marketplace in the EU for personal and non-personal data. Proposed laws include the ePrivacy Regulation, Digital Governance Act (DGA), Digital Services Act (DSA), Digital Markets Act (DMA), and the Data Act (see Table 1). These acts seek to facilitate trust in data transactions, create a more level playing field for all market players, and allow companies to share data with the government and university researchers in

[100] The United States is the world's largest supplier of semiconductor design. It has weaponized this strength against semiconductor manufacturers who supply China with chips. China, on the other hand, threatens Taiwan, which is the largest supplier of the world's most sophisticated semiconductors. Taiwan is the sole global manufacturer of certain types of semiconductors, e.g., those used in military equipment. See *The Geopolitics of Semiconductors* The Eurasia Group (September 2020).; Kathrin Hille, "TSMC: how a Taiwanese Chipmaker Became a Linchpin of the Global Economy," *Financial Times*, March 24, 2021., and; Willy Shih, "Is It Time to Rethink Globalized Supply Chains?," *MIT Sloan Management Review* 61, 4, no. Summer 2020.
[101] Farrell and Schneier, "Common Knowledge Attacks on Democracy."

service of the public interest, e.g., vaccine development. It seeks to create an ecosystem that addresses all parties in the data sharing process: business-to-business, business-to-consumer, business-to-government, and consumer-to-government, among others. In the words of the EU's chief data protection negotiator, "What we want to do in the EU through all of this regulation — and I accept that from a compliance perspective, especially if you are a small company, it must be very intimidating — but the idea is to try to create a regulatory environment where people can trust what happens online and, at the moment, they don't."[102]

The geopolitical importance of these acts is that they fundamentally challenge the historically Hayekian preferences of the US firms that dominate the European markets. They also challenge Chinese firms with global ambitions who prefer an open system outside their borders, where they can compete unfettered by Chinese Communist Party policy constraints. Since the beginning of COVID, China's big tech firms have retreated from Western markets—at least temporarily—under pressure from the Chinese government and, in the EU's case, partly due to the change in European attitudes toward doing business with them. The quiet demise of the EU-China Comprehensive Agreement on Investment (CAI), signed in December 2020, is evidence of mutual retrenchment.

While the Data Act, the Digital Services Act, and the Digital Markets Act are most certainly topics of conversation among government officials, US firms are particularly engaged in influencing policy outcomes. Companies like Microsoft and Apple have gone on a charm offensive with the EU, declaring that data privacy is a human right. Microsoft's corporate blog

[102] "In Conversation with Mr. Gencarelli," Panel discussion at IAPP *European Data Protection Congress*, Brussels 2021.

regularly posts statements endorsing the EU's regulatory agenda, including support for the Digital Markets Act, even though it will cost the company revenue.[103] However, Apple, Google, and Facebook, whose businesses face a more significant revenue threat from the new regulation, actively lobbied against the DMA in the stringent form it was passed.[104] They cite consumer security vulnerabilities and an inability to charge for intellectual property as reasons for opposing the new law. The new rules, effective in 2023, will only apply to "gatekeeper" platforms or large companies with a market capitalization of €75 billion or more that run on one core "platform" like web browsers and social media sites. The DMA is thus expected to reshape how companies like Apple, Meta, Google, Amazon, and Microsoft manage their app stores, advertising, e-commerce, and messaging services.

[103] Rima Alaily, "Microsoft supports new rules for gatekeepers," *EU Policy Blog*, *Microsoft* May 3, 2021, https://blogs.microsoft.com/eupolicy/2021/05/03/microsoft-supports-new-rules-for-gatekeepers/.
[104] Sophie Mellor, "Apple and Google criticize the new EU Digital Markets Act that will radically change the way they have operated for the past 20 years," *Fortune*, March 25, 2022, https://fortune.com/2022/03/25/apple-google-criticize-eu-digital-markets-act/.

Name	Objective	Status	Key features
ePrivacy Regulation	Trust in data transactions	Under debate	• Updates 2002 ePrivacy regulations. • Clarifies points of the GDPR, especially on internet "cookies." • A "lex specialis" versus the GDPR, which is a "lex generalis"
Data Governance Act	Trust in data transactions	In force 2023	• "Common European data space" Intended to promote voluntary sharing of public and private sector data and personal data made available by data holders through licensed data intermediaries. • Intended for research and innovation. • Will be subservient to the GDPR.
Digital Markets Act	Regulates market power based on data	In force 2023	• Regulates large online "gatekeeper" platforms to ensure fair market competition with SMEs. • Addresses personal data and private sector data held by online platforms and originating from the users. • Prevents: pre-loading of software applications; favoring platform business over competitors in search functions; requiring payment methods that favor the gatekeeper, reusing customer data provided for a specific purpose
Digital Services Act	Updates 2000 E-Commerce Directive Regulates large online platforms	Effective 2024 (likely)	• Adopts measures to counter illegal products, services and content online; • Expands tracking-free advertising and a ban on using a minor's data for targeted ads; • Recipients of services have the right to seek compensation for damages; • Mandatory risk assessments and more transparency over algorithms to fight harmful content and disinformation
Data Act	Ensure fairness in the allocation of data value among the actors of the data economy	Passed April 2022, in consultation	• A follow-up to the Data Governance Act. • Addresses access and use of private sector data, personal data and co-generated (Internet of Things) data in circumstances for public interest; regulates contracts between data aggregators and SMEs; creates ability for businesses to switch between cloud services. • The last piece of the EU Data Strategy.

TABLE 1: EU STRATEGY FOR DATA: CREATING A TRUST-BASED DIGITAL ECOSYSTEM

When it finally passed, the GDPR was widely heralded as a standard that could meet the challenge of protecting privacy in the global digital age. In a 2017 communication to parliament and the council, the Commission advocated that "the EU should seize this opportunity to promote its data protection values and facilitate data flows by encouraging convergence of legal systems."[105] In other words, the EU explicitly sought to project its normative power globally through data governance. By establishing the world's largest harmonized data privacy region, the EU hoped to promote its human rights-based approach while simultaneously allowing easier trade flows between countries. With its recent agenda of regulating digital markets, the EU has done far more than promote data protection rules. Other large markets like India have paid close attention to the debate over the digital governance acts in the EU and are taking these as models for their legislative agenda. Those countries are engaged in a comparative exercise, looking to the US, EU, and China models as they evaluate their paths for the future. The next section turns to a broad view of these three systems.

2.5 Competing Global Frameworks

The history outlined above shows how the EU is at the forefront of digital regulation that seeks to reconcile digital technologies with citizens' rights and consumer interests. The GDPR was the first regulation that prompted the much larger initiative. While the rest of the world has gradually been implementing better data privacy and protection laws, the EU has taken a comprehensive approach to regulate the digital economy. That said, the EU has not been alone. Increasingly, it faces potential competition from China. China, too, has undertaken

[105] Exchanging and Protecting Personal Data in a Globalised World, Short.

a comprehensive approach to regulating its digital economy under the banner of cyber sovereignty with widespread global implications.

As discussed in the introduction, the United States has largely stayed out of regulating its digital sector, preferring to allow companies to drive innovation through unfettered data flows. Until recently, the US's main role in influencing data protection regulation worldwide has been as an advocate on behalf of US multinationals for less regulation, if any. While this is still largely the case, Chapter VI shows how US attitudes have shifted in the direction of the EU. Under the Biden administration, the United States has also become more active internationally by announcing its *Declaration for the Internet of the Future*.[106] A key component announced in the initiative is the need to protect privacy and human rights to promote trust in an open internet environment. The United States has also become more active in promoting a business certification mechanism, the Cross Border Privacy Rules, through which firms voluntarily comply with standards set by an independent non-profit organization.[107]

China, too, has assumed an important role. Through the International Telecommunications Union (ITU), a body of the United Nations, China has argued that national governments should manage their respective internets through, among other mechanisms, a new internet protocol.[108] Scholars have recently started to argue that a nascent Beijing Effect contests the EU's Brussels Effect.[109] The Brussels Effect would suggest voluntarily adopting EU regulations to

[106] Declaration for the Future of the Internet, (U.S. Department of State, 2022).
[107] "Cross-Border Privacy Rules Certification," BBB National Programs, accessed July 1, 2022, https://bbbprograms.org/programs/all-programs/GlobalPrivacyDivision/CrossBorderPrivacyRules.
[108] Madhumita Murgia, "Inside China's controversial mission to reinvent the internet," *Financial Times* (London), March 27, 2020.
[109] Matthew Steven Erie and Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance," *54 N.Y.U. J. Int'l L. & Pol. 1* (2021), https://ssrn.com/abstract=3810256

facilitate global trade flows. The Beijing Effect, by contrast, would argue for adopting Chinese technical standards under the desire for interoperability of physical communication devices. Because China can price manufactured communications and surveillance equipment below Western companies, it encourages the adoption of its preferred technical standards. Using Chinese equipment incentivizes countries to favor Beijing's preferences in international fora that set technical standards. Creating a coalition of countries that favor Chinese technical standards is important because once a standard is adopted through the International Standards Organization (ISO), it achieves the status of international law and is institutionally embedded. If a Chinese preferred standard were adopted, Western firms would need to reconfigure their manufacturing to conform.[110] Thus, while the Brussels Effect suggests regulatory transmission for open trade flows, the Beijing Effect suggests norms transmission through technical standards. China achieves this transmission through its Belt & Road Initiative and its Digital Silk Road.

Like the EU, China initially designed its data governance legislation to fulfill domestic needs. However, over time officials realized that by exporting physical equipment and establishing its platform businesses overseas, it has an opportunity to export some of its regulatory and technical standards preferences. Rui Ma, the creator of the *Tech Buzz China* podcast, helpfully divides China's regulatory initiatives into three categories: 1) Chinese idiosyncratic, 2) keeping up with the West, and; 3) standards setting for new technology rules.[111] China's data governance falls into the latter two categories.

[110] Laura DeNardis and Michael Murphree, "Digital Standards," *Digital Economy & Security Collaborative*, February 17, 2022.
[111] *The Sound of Economics*, podcast audio, Why is China Cracking Down on Big Tech?, https://audioboom.com/posts/7976991-why-is-china-cracking-down-on-big-tech.

Some scholars have even warned about the possibility that China would like to seek to export its model of governance. What the "China model" is and how transferrable it is to environments outside of China is a subject of considerable academic debate.[112] Nevertheless, the size of China's economy and the depth and breadth of its trading relations, especially with developing countries, have opened up a huge opportunity set for China to exercise its external influence in the technology standards space.[113]

As a result of these developments, we can loosely divide global data governance into three broad approaches: the United States, China, and the EU. Until recently, the European model dominated the landscape, with the United States as an outlier, although not without its influence. The UN UNCTAD has generated a visual image (Figure 1) to demonstrate the differences.

FIGURE 1: DATA GOVERNANCE APPROACH

source: UN UNCTAD *Digital Economy Report 2020*

[112] Cf. Naughton, Barry. (2010). "China's Distinctive System: Can it be a Model for Others?" *Journal of Contemporary China* 19(65): 437-460. See also Breslin, Shaun. (2011). "The 'China model' and the global crisis: from Friedrich List to a Chinese mode of governance?" *International Affairs* 87(6): 1323–1343.

[113] A fascinating example is Senegal, which as a signatory of the Convention 108+ has adopted European data protection standards but planned to house all government data on a cloud servers run by Huawei of China. Cf. Jan van der Made, "Senegal to move all government data to Huawei-run data center," (June 25, 2021). https://www.rfi.fr/en/africa/20210625-senegal-to-move-all-government-data-to-huawei-run-data-center-china-africa-macky-sall-information-technology.

The above picture is a useful heuristic for understanding the different approaches and means through which these actors seek to externalize their preferences. The reality is, of course, more complicated. Since Russia invaded Ukraine, EU and US officials have accelerated their cooperation on multiple fronts. For example, the long-standing dispute between the EU and US on cross-border data transfers (to be discussed in Chapter VI) was ultimately raised to the level of the presidency and finally resolved, at least in principle, in March 2022. Another example is the EU-US Tech and Trade Council (TTC), which started last fall as an initiative to iron out many of the differences between the EU and United States on data governance and technology-related policy but has since become focused on the implications of the Ukraine war for the technology sector and supply chains related to it.[114] The war has brought significant commonalities between the two parties into relief. In particular, EU-US coordination on export restrictions has played an important role in stunting Russia's war efforts.[115] They have also demonstrated to China the dangers of pushing its techno-authoritarian model too aggressively. As a result, a new window of opportunity for the EU to diffuse its data privacy regulation preferences worldwide has opened in recent months. The next chapter discusses the theoretical frameworks through which the EU's preferences are projected around the world.

[114] "U.S.-E.U. Trade and Technology Council (TTC)," Office of the United States Trade Representative, accessed June 4, 2022, https://ustr.gov/useuttc.
[115] "US, UK and EU Impose Significant Sanctions and Export Controls in Response to Russia's Invasion of Ukraine," Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, updated February 26, 2022, accessed June 4, 2022, https://www.skadden.com/insights/publications/2022/02/us-uk-and-eu-impose-significant-sanctions.

3 Chapter III: GDPR Diffusion Channels

3.1 Introduction

The last chapter introduced the broader context of the GDPR and the goals of the EU's digital strategy. This chapter sketches out the channels through which the GDPR is diffused. The chapter begins with a brief overview of competing instruments used to facilitate cross-border data flows. The most important of these is the EU's adequacy status, which has been lightly referenced until this point and needs further explanation. Second, the chapter outlines two theoretical frameworks that describe the political dynamics created by the GDPR and the mechanisms through which it generates or coerces regulatory convergence. The theoretical frameworks fleshed out here include the Brussels Effect and the New Interdependence Approach (NIA). These descriptions form additional building blocks for understanding the case studies. Both the frameworks and an understanding of the institutional mechanisms of diffusion help delineate the limits of the EU's ability to project its power and European values through data protection regulation.

3.2 EU Adequacy and other Systems of Cross-border Data Transfer

Colin Bennett observes that transnational instruments for data protection have played three overlapping functions. They have acted as *instruments of harmonization*, i.e., as templates that any state or organization might use to fashion its own data protection policy. They have acted as *exemplars*, "producing a progressive and inexorable desire to be within the community of nations that has adopted data protection legislation." This is true, for example, in the case of Colombian regulators and other countries that have sought to create the legal

conditions through which they can apply for EU adequacy status. As an exemplar gains traction around the world, pressure grows on the non-adopters to raise their standards. More recently, transnational instruments have acted as a *coercive force*, with significant economic consequences for those businesses that rely upon the unimpeded international flow of personal information and on those governments that wish to protect their domestic industries from the possible consequences of non-compliance. The EU's adequacy status is one of the coercive instruments to the degree that EU officials can compel legislative change in jurisdictions outside the EU.

Consistent with the narrative in the previous chapter, Bennett further argues that these instruments have built upon each other over time. They represent a logical progression reflecting the increasing policy interdependence of different countries. The EU's 1995 Data Protection Directive (DPD) was only possible because of prior agreement on data protection principles within the OECD. By the same token, the GDPR was only possible because of twenty years of experience through the Directive. "The GDPR," he says, "is clearly a significant extension of the global process of policy convergence and trading up the of international privacy standards. The criteria for convergence are deepening."[116]

Woven throughout the narrative of transmission mechanisms and transnational instruments is the concomitant change in attitudes toward data privacy as the digital world grew from minimal to omnipresent in those countries where internet access is widespread. While there is an identifiable causal chain in the transmission mechanisms, the secular trend toward

[116] Colin J. Bennett, "The European General Data Protection Regulation: An instrument for the globalization of privacy standards?," *Information Polity* 23 (2018), https://doi.org/10.3233/IP-180002.

digitization has called attention to the need for data privacy regulation. Privacy activists worldwide, such as the Future of Privacy Forum, Access Now, and EPIC, collaborated and promoted their message at international venues to generate a shift in global attitudes. Whereas cultural attitudes toward privacy vary from country to country, the growing numbers of cyberattacks, ransomware cases, and abusive spamming practices have incentivized better privacy protections and data protection.

A key example of this shifting trend is the Council of Europe's (CoE*) Convention 108,* a legally binding global treaty signed in 1981 by European nations that set a global minimum standard for data protection.[117] The Convention 108 is similar to the OECD principles discussed in Chapter II. While initial signatories were all European nations, the CoE explicitly set out to globalize its data protection standards in the early 2010s. Uruguay was the first non-European nation to accede to the Convention 108. Since then, an additional 13 non-European nations have either signed or acceded to the Convention 108 in addition to Uruguay. The list of acceding nations shows the global scope of shifting attitudes toward the need for data governance: Argentina, Azerbaijan, Burkina Faso, Cape Verde, Georgia, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Turkey.

The CoE promotes the *Convention 108* through its Consultative Committee, which is responsible for interpreting the Convention's provisions and for monitoring its implementation. Observers play the key role of reporting on events at the CoE to their organizations. It is

[117] The Council of Europe is Europe's oldest political body, aims to uphold human rights, democracy and the rule of law across the continent. There is considerable overlap between the work and objectives of the EU and the Council of Europe. Founded in 1949, the Council has 46 member states, covering a population of approximately 750 million. All European countries are now members apart from Belarus, which lacks adequate human rights protections, and Kosovo, whose independence is not recognized by all Council of Europe members. Since the invasion of Ukraine, Russia dropped out of the Council of Europe to avoid being suspended.

composed of representatives of parties to the Convention and observers from other States, international organizations, and NGOs.[118] The interplay of the EU's GDPR standards and the CoE *Convention 108* is of note. One week before the GDPR took effect in 2018, the CoE undertook to update the Convention, now referred to as Convention 108+, to bring it closer to compliance with the GDPR. Today, the adoption of the Convention 108+ is widely perceived as putting a country on the path to attaining EU adequacy status.

Besides the Convention 108+, there is an alphabet soup of regional data governance arrangements, including the African Union Convention, the Standards for Personal Data Protection for Ibero-American States with Latin American signatories, and the Asia-based APEC Cross-Border Privacy Rules system. None of these rises to the rigor of the GDPR and do not exercise a high level of influence beyond their regions. In Asia, for example, the APEC Cross-Border Privacy Rules (APEC CBPRs) have provided a blueprint for a common regional approach. Thus far, there are nine signatory nations to the APEC CBPRs, including Australia, Canada, Japan, S. Korea, Mexico, the Philippines, Taiwan, Singapore, and the United States. The APEC CBPRs comprise a non-binding scheme with no enforcement mechanism although countries must demonstrate that they can enforce its rules.[119] The United States has been an active promoter of the APEC CBPRs because it prefers self-regulatory instruments to highly prescribed ones like the EU's GDPR. None of the APEC countries has standards as low as those specified by the APEC CBPRs, a sign

[118] "Consultative Committee," Council of Europe, accessed June 4, 2022, https://www.coe.int/en/web/data-protection/consultative-committee-tpd.
[119] https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

that such voluntary instruments lack rigor.[120] To add greater accountability, the United States and others have proposed adding independent bodies to audit the self-certification process.

More recently, bilateral and multilateral trade agreements have started to include robust digital chapters that were brief and insubstantial in prior decades. Key examples of multilateral agreements with substantial digital chapters include the Regional Comprehensive Economic Partnership (RCEP), which took effect in 2022, and the Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP).

3.3 EU Adequacy Status

What differentiates the EU's adequacy status from the instruments above primarily lies in the enforcement mechanisms. Adequacy findings are granted by the European Commission when countries undergo a consultation process with the EU data privacy officials to establish the extent to which their legal system adequately protects citizen data. In particular, the EU is focused on EU citizen data. If the third country's laws are deemed sufficiently protective by EU standards, businesses in those countries can freely transfer EU citizen data to that country outside the EU. Note that the directional flow is from the EU into other countries. It is not bidirectional.

In *traditional adequacy findings*, the EU has been the more powerful negotiating body and exercises a certain degree of coercive power over its interlocutor. For example, almost all countries must amend existing legislation to bring it closer to GDPR regulations if they wish to have a favorable adequacy finding. The exception to this is the agreement reached with the

[120] Greenleaf, Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi.

United States, which is better characterized as a *concessionary agreement* than a traditional adequacy finding, as evident in the United States case study.

3.3.1 Background

The 1995 DPD first introduced the concept of adequacy decisions to streamline compliance with the directive for companies outside the European Economic Area (EEA) doing business with it. The effect of an adequacy finding is, "that personal data can flow from the EU … to [a] third country without any further safeguard being necessary. In other words, transfers to the country in question will be assimilated to intra-EU transmissions of data."[121] Except for the UK, these adequacy decisions do not cover data exchanges in the law enforcement sector, which are governed by the Law Enforcement Directive. Without an adequacy finding, individual companies must rely on standard contractual clauses (SCCs) or binding corporate rules (BCRs) to effect cross-border data transfers. SCC and BCRs are an expensive and cumbersome imposition. For further details, refer to Appendix 3.

The Commission's primary consideration when making an adequacy decision is the extent to which the third country's law offers the same protections for personal data and the rights of data subjects as provided under European law.[122] The Commission's leeway in determining adequacy was considerably narrowed in 2015 due to the European Court of Justice ruling in *Maximillan Schrems v. Data Protection Commissioner (Ireland)* ('*Schrems*'). Before 2015, the Commission held that it was unnecessary for a third country to offer the same level of data

[121] "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection," European Commission, accessed July 5, 2021, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[122] "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection."

protection as the Directive. It was sufficient that the country offered a broadly similar level of protection, even though it extended a lower level of protection than the EU in some minor respects. However, the court held in a second ruling, *Schrems II,* that while a country's law does not need to be identical to EU law to be considered adequate, it must ensure a level of protection of personal data and the rights of data subjects that is "*essentially equivalent*" to that guaranteed in the EU by the Directive. Essentially equivalent means that the laws of a country must achieve the same privacy and dignitary outcomes. Indeed, EU member nations do not have identical data protection laws.[123] Some countries, like Germany, have stricter standards than the GDPR in given sectors. In this sense, the GDPR can be considered the minimum acceptable standard among EU member states.

To date, 15 countries have been extended adequacy status. Many observers lament the high threshold for adequacy and the length of time it takes to secure an adequacy finding from the EU. They cite these as factors explaining why more countries have not sought adequacy. Appendix 3 provides details on the decision process.

3.3.2 Adequacy and Academic Literature

Academic literature on adequacy status is limited. Most articles are written by law firms or published technical journals for legal practitioners interested in compliance.[124] For example, Maarja Saluste offers a detailed discussion of the specific bureaucratic entities involved in the

[123] One can think of the EU regulation in the same way that the United States has federal laws that *preempt* state laws. US laws that preempt state law impose a minimum standard below which states cannot fall.
[124] Cf. Paul Von dem Bussche Axel Voigt, "The EU General Data Protection Regulation (GDPR) : a Practical Guide," (2017), https://doi.org/10.1007/978-3-319-57959-7. See also Xanthoulis, *Negotiating the EU Data Protection Reform: Reflections on the Household Exemption*, 441; W. Gregory Voss, "CROSS-BORDER DATA FLOWS, THE GDPR, AND DATA GOVERNANCE," Article, *Washington International Law Journal* 29, no. 3 (2020).

process of determining adequacy and their requisite obligations.[125] Greenleaf extensively documents older adequacy findings and shows where they fall short of the GDPR standards.[126] One explanation for the lack of theoretical literature on adequacy is that consultations are confidential, and the public only sees the final adequacy findings. For example, there are virtually no public statements by the EU and Japan discussing their adequacy negotiation process.

From an IR theoretical perspective, the EU's market power can historically explain adequacy findings. This explanatory power still holds for many countries. However, since the passage of the GDPR in 2016 and the rise of the digital economy as a vital geopolitical force, a wider variety of motivations explains why countries would seek EU adequacy status. Since the GDPR took effect in 2019, Japan, Korea, and the UK have attained adequacy status. The United States is near reestablishing its adequacy since U.S. President Joe Biden issued an executive order in October 2022 as one condition of a new agreement.[127] The Japan case study will show that the adequacy agreement between the EU and Japan came about as a confluence of factors that reflected broader strategic goals on both sides rather than merely the EU exercising unilateral coercive power.

Little work is devoted to the theoretical or geopolitical significance of adequacy findings. Farrell and Newman's NIA uses the example of the EU-US Privacy Shield—which yielded an EU adequacy decision—as a case study for their theory. The NIA is appropriate to the EU-US model,

[125] Maarja Saluste, *Adequacy decisions: an opportunity for regulatory cooperation on data protection?* (2021).
[126] Greenleaf, Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi.; Graham Greenleaf, "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance," in *169 Privacy Laws & Business International Report, UNSW Law Research Paper No. 21-60* (University of New South Wales, 2021).
[127] That executive order is now under review by the European Data Protection Board and the European Commission for is compliance with the "essential equivalence" requirement defined by the European Court of Justice.

which is discussed in the next section. However, most adequacy findings before the GDPR were with countries that, unlike the United States, were considerably smaller than the EU and therefore had little bargaining power. Countries that attained conventional adequacy findings before the GDPR included: Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, New Zealand, Switzerland, and Uruguay.[128] This list demonstrates how much more dominant the EU was in these negotiations from an economic perspective. Because of the EU's dominance, a case can be made that market power theories best explain these findings. That is a topic for research beyond the scope of this thesis.

Since the first Schrems ruling and the passage of the GDPR, the EU's standards have tightened considerably. In this sense, attaining adequacy has grown more exacting and arguably more coercive for adopting countries. In this sense, adequacy as a data transfer instrument starkly contrasts the soft power emphasis described in the Brussels Effect. The Brussels Effect is the topic of the next section.

3.4 The Brussels Effect

The Brussels Effect is a theoretical model developed by Anu Bradford to explain the European Union's superpower status as a global regulator. It conceptually encapsulates the EU's ability to encourage voluntary adoption of its regulations in the process of regulating its own Single Market. Bradford applies this model to a range of cases, including global competition law, consumer health and safety, environmental standards, and digital regulation.

[128] "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection."

Adoption of EU regulations can occur at the country level, as in the example of Colombian regulators who are currently putting a data governance structure in place that would position the country for adequacy status in the future.[129] Adoption can also occur within the private sector when, for example, global companies opt to universalize GDPR standards across their global platform after having done so to comply with the EU portion of their business. This might be referred to as a spillover effect in which the EU is hands-off and plays a background role in the adoption of the standards.[130]

Bradford defines the Brussels Effect as the EU's "ability to shape the international regulatory environment without the need to resort to coercion or cooperation."[131] As such, there is no push factor from the EU toward other countries. The term generally captures the "phenomenon where the markets are transmitting the EU's regulations to both market participants and regulators outside the EU."[132] It builds on a large body of work on regulatory competition and convergence, including the pathbreaking work by David Vogel on the California Effect. The California Effect is the shift of consumer, environmental, and other regulations in the direction of political jurisdictions with stricter regulatory standards. The name is derived from the spread of advanced environmental regulatory standards originally adopted by California and eventually adopted in other US states. This spread is supported by large corporations, which stand to gain

[129] FIP Luis Alberto Montezuma, "Obtaining adequacy standing for Colombia," (August 2, 2018). https://iapp.org/news/a/obtaining-adequacy-standing-for-colombia/.
[130] Spillover is core concept in neo-functionalist theories of European integration with several different strands that reach beyond the scope of this discussion. See Ernst B. Haas, *The Uniting of Europe* (Stanford: Stanford Univ. Press, 1958). See also Alec Stone Sweet, Wayne Sandholtz, and Niel Fligstein, *The Institutionalization of Europe* (Oxford: Oxford University Press, 2001).
[131] Anu Bradford, " The Brussels Effect and China: Shaping Tech Standards: Insights from Anu Bradford," interview by Mercy Kuo, 01/07/2021, 2021, https://thediplomat.com/2021/01/the-brussels-effect-and-china-shaping-tech-standards/.
[132] Anu Bradford, *The Brussels Effect* (Oxford: Oxford University Press, 2020)., pp. 1.

from the harmonization of rules across jurisdictions. This process is the opposite of the Delaware effect, or the "race to the bottom," in which different countries (or US states) reduce their regulatory burden to attract more businesses into their jurisdiction. The assumption behind the Delaware effect is that governments reduce regulatory barriers in the competitive regulatory environment to attract new companies to establish business in their jurisdiction. When businesses lobby for weaker regulations by threatening to move their operations to more "business-friendly" jurisdictions, this is often called regulatory arbitrage.

Bradford also builds on the extensive work of Abraham Newman. Newman's 2008 book, *Protectors of Privacy,* compares the US and EU approach to data protection regulation. Newman traces the global move toward more comprehensive data privacy regulation away from the more limited US-led model and shows how, by 2008, the EU had developed enough institutional regulatory capacity to impose its approach upon other countries. Newman argues that market power, although a critical factor in explaining the ability to diffuse regulation globally, must be complemented by strong institutional structures in command of subject matter expertise and sufficient supervisory capacity to buttress enforcement. Market power in this context should not be confused with market forces. The former reflects a country's ability to gain concessions from another country as a condition of access to its large consumer market. Market forces are driven by actions of the private sector that bring about change.

In *The Brussels Effect*, Bradford responds to critiques of globalization as a driver of a regulatory "race to the bottom," by which countries lower their regulatory standards to increase their relative competitiveness in the global economy. *Raising global standards is a key analytical condition of the BE.* Bradford shows through case studies that instead of lowering global

standards as predicted by theories of regulatory arbitrage, the EU's regulation in fact raises global standards. The GDPR is a strong example of this dynamic at work and is corroborated by the empirical work by Greenleaf.[133]

The preconditions for the Brussels Effect to occur include: strong global market power, regulatory capacity (subject-matter expertise and institutional depth); relatively high standards; inelasticity of the relevant consumer market, and companies' preferences for uniformity.[134] These features create the condition of the possibility of the Brussels Effect to occur. The analytical conditions for evaluating whether the Brussels Effect has occurred or failed are *voluntary adoption* and *independence of the adopting country or firm's relationship with the EU*.[135] In sum, the Brussels Effect occurs when third countries adopt higher European standards voluntarily and independently of their relationship with the EU.

3.4.1 Voluntary Adoption Condition

A commonly observed instantiation of the Brussels Effect is through corporations that do business with and in the EU. As the EU regulates its single market of 450 million citizens, global corporations complying with the GDPR in Europe voluntarily elect to adopt those rules across their global platform and thereby transmit EU rules across the global marketplace. In this case, the first instantiation of GDPR adoption is based on requirements for market access. However, the follow-on adoption of standards across a global platform represents the voluntary

[133] Greenleaf, Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi.
[134] Bradford, *The Brussels Effect*. See pages 25-66.
[135] Bradford, interview.

component. For example, Microsoft and Google extended GDPR standards across their global platform once it was implemented in Europe to comply with the local mandate.

Having adopted GDPR standards, corporations become incentivized to advocate for a level playing field across the globe and will in turn pressure their home country regulators to adopt European standards. In this case, the policy transmission flows from corporations to states (from *de facto* to *de jure*) rather than the other way around. An oft-mentioned example of the GDPR's ability to shape corporate thinking are quotes from both Brad Smith, CEO of Microsoft, and Tim Cook, CEO of Apple, who were both quoted in global media as saying they believe "privacy is a fundamental human right."[136] Since Microsoft implemented GDPR standards across its global platform, it has become a powerful advocate for both global data privacy standards and the development of so-called "cyber-norms." In 2018, for example, Microsoft co-authored an initiative with the French government entitled the *Paris Call for Trust and Security in Cyberspace*.[137]

More recently, Apple's adoption of more consumer-friendly privacy settings in line with GDPR led Facebook to attribute a $10bn decline in quarterly revenues for third quarter 2021 earnings.[138] In April 2021, Apple specifically adopted European privacy default settings, which turn off IDFA, or identifiers for advertisers. Users are now explicitly asked to turn on data collection settings to allow advertisers to track the performance of their ads and to target ads at

[136] Schwartz, "GLOBAL DATA PRIVACY: THE EU WAY."
[137] Bradford, pp. 144, and L. M. Hurel and L.C. Lovato, ""Cyber-Norms Entrepreneurship? Understanding Microsoft's Advocacy on Cybersecurity"," in *Governing Cyberspace: Behaviour, Power, and Diplomacy*, ed. D. Broeders and B. van den Berg (London: Rowman & Littlefield, 2020).
[138] Sheila Dang and Nivedita Balu, "Facebook ad revenue seen feeling brunt of Apple privacy changes," October 25, 2021. https://www.reuters.com/technology/facebook-ad-revenue-seen-feeling-brunt-apple-privacy-changes-2021-10-25/.

users.[139] This corporate advocacy dynamic demonstrates how the EU exerts a passive but deep influence on corporate behavior, transforming global markets in the process. In the case of US corporations, the shift toward embracing a dignitary approach to data privacy at the expense of the purely economic approach is a sea change. Some companies now see strict data privacy standards as a form of competitive advantage.

Extension of GDPR at the company level can also occur across two directions. Vertical extension occurs when firms roll out GDPR standards across a global platform, as discussed previously. Microsoft and Apple are examples of vertical transmission of GDPR standards. Horizontal transmission of GDPR standards also occurs when vertical adopters require their suppliers to comply with GDPR standards as well. Horizontal extension sometimes occurs as a function of the EU's standard contractual clauses (SCCs), which are the legal mechanism through which data transfers occur in the absence of state-to-state arrangements like adequacy status. SCCs will be discussed below. Through both vertical and horizontal penetration, the standards can reach high penetration at the *de facto* level. (For more on SCCs, see Appendix 3.)

An alternative transmission mechanism of the Brussels Effect is through states or at the *de jure* level. It occurs when EU standards serve as templates for foreign nations leveraging European regulatory expertise and capacity. In this context, countries can sometimes adopt higher regulatory standards against the wishes of corporations. Brazil and China are two examples of the *de jure* Brussels Effect. The China case study will show that the domestic dynamics played and continue to play a decisive role in how and why the GDPR is adapted to the local setting. Research by Tao Fu, for example, showed that Chinese corporations have preferred weaker

[139] https://www.siliconrepublic.com/business/apple-privacy-facebook-snapchat-cost

rather than stronger data protections for consumers.[140] China's regulators have overridden private corporate preferences. In the case of China, the EU standards combine statutory precision with flexible drafting, a principle that is inherently appealing because of the Chinese legal tradition which favors flexibility in interpretation.[141]

3.4.2 Independence Condition

A second condition of the Brussels Effect is that firms or countries adopt GDPR *independent of their relationship with EU*. Adoption is not the product of a cooperative arrangement, such as a free trade agreement (FTA), a preferential trade agreement (PTA), or a multilateral agreement. While trade agreements and the adoption of GDPR standards may occur in tandem, they are not causally linked. Thus, trade agreements may be complementary in nature. In summary terms, the Brussels Effect is distinguished from trade agreements by three factors. First, trade agreements are formal government-to-government arrangements driven largely from the top-down but in consultation with civil society actors. Second, a critical component of EU treaties is the stated desire to project the EU's norms and values on the wider world.[142] Since the stalemate in the WTO Doha Rounds, the EU has moved more aggressively to pursue a normative agenda with its trading partners. Under the Brussels Effect, however, the desire to transmit norms is implicit and not a stated intention. Third, trade agreements involve the approval of the legislative bodies of both trading partners, which is often wrought with political

[140] Tao Fu, "China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent," *Global Media and Communication* 15 (05/27 2019), https://doi.org/10.1177/1742766519846644.
[141] Rogier Creemers, "Party Ideology and Chinese Law," in *Law and the Party in China: Ideology and Organisation* (Cambridge: Cambridge University Press, 2021).
[142] Stated by the EU in the Treaty on the Functioning of the EU (TFEU).

stresses that make treaties hard to pass. The independence condition can be better understood by seeing it in a contextual example.

3.4.3 Example: EU Environmental Regulation Diffusion

There is some academic literature exploring the influence of the EU on China with respect to climate change policy that is a tempting analogy for assessing diffusion within the data privacy context.[143] While the EU's leadership role in climate change dialogue is undisputed, the question is whether the Brussels Effect accurately describes how EU attitudes towards environmental regulation are transmitted. Climate change has been high on the EU's agenda with China in meetings for over a decade now. Because so much of the climate change discussion has taken place at the high levels of government and pledges to meet global carbon emissions targets have occurred through multilateral fora such as the Kyoto (1995) and Paris Climate Accords (2015), we can argue that the Brussels Effect for the does not apply. Were it to apply, China would have adopted the EU's carbon emissions standards *independent* of its relationship with the EU instead of being a condition of certain agreements. This has clearly not been the case. For example, China threatened to halt Airbus orders in retaliation for the EU's attempt to require all aircraft to purchase emissions permits for flights landing in or departing from European airports.[144] Although one might be able to document individual instances of the Brussels

[143] See, for example, Astrid Carrapatoso, "Climate policy diffusion: interregional dialogue in China–EU relations," *Global Change, Peace & Security* 23, no. 2 (2011/06/01 2011), https://doi.org/10.1080/14781158.2011.580959, https://doi.org/10.1080/14781158.2011.580959.
[144] Bradford, pp 219.

Effect in China's environmental regulations, for example, in the case of animal testing in cosmetics production, there is little evidence of it on China's climate change policy writ large.[145]

Summarizing the Brussels Effect as a mechanism, its core features are voluntary and independent adoption of EU regulatory frameworks. The other core feature is that the Brussels Effect raises regulatory standards. It explains the opposite outcome of the Delaware Effect, which suggests a regulatory race to the bottom as a function of corporate jurisdictional arbitrage. The Brussels Effect is, therefore, a globalized adaptation of Vogel's California Effect, a theory describing the adoption by other US states of California's more stringent environmental rules. By virtue of these features, the EU's ability to ensure the human rights or dignitary underpinnings of the GDPR or any other standards-raising frameworks is largely limited. This does not mean that the EU cannot encourage them through other means or perhaps in concert with the Brussels Effect. One of the implicit assumptions of the Brussels Effect is that the EU's regulatory frameworks win the marketplace of ideas. There is no excluding conceptual spillovers, which can hold true even for illiberal regimes. The China case study evaluates this question in detail.

3.5 The New Interdependence Approach

3.5.1 NIA in brief

Whereas the older IR theories of realism and neoliberalism endeavor to explain the world that brought about globalization, the NIA seeks to explain the world order that globalization has created. Three core ideas are central to the NIA. First, globalization does not occur in a

[145] Bradford highlights the example of Japanese companies voluntarily halting animal testing in cosmetics, but still following Chinese rules that required animal testing of cosmetics. In 2014, the Chinese government dropped this requirement, and Japanese companies then followed suit by selling non-animal tested make up in China (Bradford 2020, pp 216-217).

state of anarchy—one held in check by sovereign states—but in a state of *rule overlap*. Interactions across borders mean that actors become aware of differences in domestic regulations that interfere with and influence each other. For example, multinational corporations that bear the cost of complying with rules in multiple jurisdictions lobby heavily for the harmonization of rules that ensure business visibility and reduce the cost of compliance. At times, these businesses will sacrifice their preferred rules in favor of a harmonizing arrangement. The uncertainty caused by rule overlap and clash offers openings for change actors to disrupt embedded institutions they do not like. By extension, status quo actors who are content with the established structures find themselves open to attack from new trajectories. [146]

Thus, a second feature of the NIA is that globalization creates *opportunity structures* for collective actors (e.g., regulators, firms, consumer groups, and international organizations) to form transnational alliances. As the authors note, during the early days of globalization, political contestation remained largely confined to the nation-state. Change actors looked to domestic channels for reform. Once globalization became established, the opportunity structures extended beyond domestic channels, and change actors could participate directly in global politics through institutions above and below the nation-state level. In this way, international institutions like the UN or the WTO, originally created by nation-states, became venues through which various actors can collaborate and coordinate to influence or change global regulations. Moreover, professional conferences, such as the many privacy and data protection conferences that take place worldwide, attracted corporate, regulatory, and civil society participants who share information, coordinate their advocacy, and seek solutions to given problems. Therefore,

[146] Farrell and Newman, *Of Privacy and Power*. Pg. 27-30.

solutions are driven less by functional imperatives, e.g., achieving data flows for market efficiencies, and come to incorporate a wider variety of objectives. Successful solutions depend on the organizational and executive capacity of the collective actors. Through this mechanism, power is redistributed away from the state and partially reallocated to corporations, regulators, international organizations, NGOs, and the like.[147]

Third, institutions are a key source of *asymmetric power*, not just as rules of the game. Institutions shape the power of actors as well as their understanding of preferences.[148] As Farrell and Newman show, the Safe Harbor agreement between the US and the EU was negotiated on a state-to-state basis from which privacy activists and regulators who sought to defend European privacy rules were precluded. This concessionary agreement "provided US e-commerce companies with the institutional means to superficially satisfy EU regulators while developing business models that were at odds with the value of Europe's privacy regime."[149] Through access to key institutions, actors can engage in a strategy of what Farrell and Newman have called *defend and extend*. This is a core argument of their theory.

3.5.2 Defend and Extend

In brief, defend and extend encapsulates the idea that collective actors who have access to transnational forums will use them to defend the status quo of their domestic institutions if this is their preferred outcome. They seek to extend the reach of their domestic institutional frameworks to other countries along the lines suggested by Daniel Drezner.[150] They do so in

[147] Farrell and Newman, *Of Privacy and Power*. Pgs. 29-30.
[148] Henry Farrell and Abraham Newman, "The new interdependence approach: theoretical development and empirical demonstration," *Review of International Political Economy* 23, no. 5 (2016/09/02 2016), https://doi.org/10.1080/09692290.2016.1247009.
[149] Farrell and Newman, *Of Privacy and Power*. Pgs. 126-127.
[150] Drezner, "All politics is global : explaining international regulatory regimes."

order to shift the adjustment costs of any rule conflict to the other jurisdiction. The authors cite examples from both the US and the EU to show how states sought to access international venues to extend their policy preferences. In the case of the US, this was its preference for rules about insider trading in the US stock market. A bright example from the EU was its efforts to export its high standards on airline carbon emissions and food standards. Europe's data privacy regulators have actively sought to defend and extend their preferences worldwide.

3.5.3 Cross-National Layering

Collective actors who wish to overturn the status quo and have access to the relevant transnational forums adopt a different approach but use the same mechanism. Rather than using international venues to defend their domestic institutions, they create cross-national alliances that can undermine domestic institutions over time to generate change. The authors build on the work of Kathleen Thelen and others who describe a domestic variant of domestic institution-building used to overturn the status quo.[151] Applied in the international context, "transnational institutions can become a source of endogenous change within national jurisdictions." Once transnational institutions establish a foothold, they can influence other institutions or rules. Over time, the transnational agreement subsumes or replaces domestic rules by making them less and less relevant to reality on the ground. Support for and compliance with transnational agreements reshapes the incentives of domestic collective actors who were previously inclined to block change.[152]

[151] Kathleen Thelen, "HOW INSTITUTIONS EVOLVE: INSIGHTS FROM COMPARATIVE HISTORICAL ANALYSIS," in *Comparative Historical Analysis in the Social Sciences*, ed. Dietrich Rueschemeyer and James Mahoney, Cambridge Studies in Comparative Politics (Cambridge: Cambridge University Press, 2003).
[152] Farrell and Newman, *Of Privacy and Power*. Pg. 32-33.

3.5.4 NIA Application

The *concessionary agreements* struck between the EU and the US to achieve a positive adequacy finding is explained by the NIA. Both the EU and the US sought to defend and extend their models to the other jurisdiction. But because the two jurisdictions sought to avoid a confrontation, a hybrid concessionary arrangement was a necessary outcome. As Farrell and Newman extensively document in their book, the Privacy Shield of 2018 was the second of two data sharing arrangements between the EU and the US and was struck months before the GDPR took effect. The agreement replaced the Safe Harbor Agreement, which was struck down by the European Court of Justice (ECJ) in 2015.

Like its predecessor, the Privacy Shield required the EU to turn a blind eye to a gross lack of data privacy protection at the US federal legislative level. By European standards, there was nothing adequate about data protections in the United States. Whereas in traditional adequacy findings, the adopting country would change its legal system to accommodate EU requirements, the United States did not. As such, the United States was successful in defending its existing institutions. As a compromise, the EU obtained concessions from the US that would allow for better enforcement of privacy protections for EU citizen data transferred outside of EU borders. Thus, the EU could claim that they protected their existing institutions by dictating the terms of the US's self-regulatory data privacy system.

Since the GDPR took effect and the EU-US concessionary agreements have been definitely ruled out by the ECJ, the EU holds the upper hand for the time being. It has not only defended, but will potentially have extended its framework to the United States, as the case study will show.

3.6 Comparing the Brussels Effect and the NIA

The Brussels Effect and the NIA both seek to describe the influence of one set of policy preferences on another country in ways that extend beyond traditional static IR frameworks. In considering the two theories side-by-side, one can differentiate them by the direction of their influence. The Brussels Effect is largely uni-directional, pointing from the EU out to the rest of the world. It is also, as mentioned previously, definitionally based on voluntary adoption independent of the adopting country's relationship with the EU. The NIA describes a more dynamic approach in which parties mutually influence one another. This NIA does not broadly comment on voluntary versus coercive methods. In the case study of the EU-US, it is clear that both parties mutually influenced one another, not just in the course of negotiations but over a long trajectory of more than a decade.

Both account for the influence of civil society parties, but the NIA more actively considers these actors' role. While the Brussels Effect largely discusses the role that businesses play in arguing to raise standards, it pays less attention to transnational institutions and NGOs. By contrast, the NIA accounts for NGOs and other civil society actors in its theoretical narrative. Finally, the NIA is agnostic on raising or lowering standards. While it extensively documents the negotiations around data-sharing, it is more focused on the process rather than the nature of the change.

Having considered the theoretical foundations of GDPR transmission, the application in the case studies follows.

4 Chapter IV: China & the Brussels Effect as part of Recentralized Authoritarian Capitalism

4.1 Introduction & Theoretical Approach

On August 20, 2021, China passed its long-anticipated Personal Information Protection Law (PIPL). Along with the Cybersecurity Law (CSL) implemented in 2017 and the Data Security Law passed in June 2021, the PIPL is regarded as a major milestone in China's multi-year legislative efforts to establish comprehensive regulation on data governance at the national, firm, and individual levels. The PIPL is a response to a constellation of domestic and international factors, including Xi Jinping's strategic vision of China as a "cyber-superpower" and Chinese consumer calls for data privacy protections in the wake of data theft that resulted in widespread financial fraud.[153] The PIPL draws considerably from the European Union's GDPR and frequently invites comparison.

This chapter investigates the overlaps and divergences of the PIPL and the GDPR and frames them within the Chinese context. It shows how the Brussels Effect framework applies to China as an adaptation of the GDPR. It is a research puzzle to explain why China would adopt these standards based on the EU's Charter of Fundamental Rights. This chapter will examine the extent to which China has adopted GDPR concepts, standards, and privacy protection practices by comparing similarities and differences between the two and relating them to China's broader policy objectives.

[153] Adam Segal, "When China Rules the Web," *Foreign Affairs*, no. Sept/Oct 2018 (2018), https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.

However, the Brussels Effect alone does not comprehensively explain the adoption of GDPR-like data protection rules. Complement its explanatory power is a synthesis of scholarship from Rogier Creemers, Chiu-Wan Liu, Andrew Mertha, Margaret Pearson, Rithmire and Chen, and Dali Yang, among others. The core argument is that China has adopted the PIPL as a tool to rein in the private sector and better define the narrow space for civil society. Announced two weeks before the PIPL was passed, China's infamous 2021 tech crackdown is striking evidence of how China has wrapped data governance regulation and government control into the mantel of market competition. Some of this is legitimate and reflects similar moves taken by the EU. Based on their scale alone, China's large digital platforms are easily vulnerable to accusations of anti-competitive practices. However, because so many of China's digital platforms also deliver consumer credit and other financial services, this has made them a target of government intervention on yet another front. The sheer scope and scale of China's digital economy, and the enormous role that a small handful of private sector companies plays in China's economy has prompted a step beyond China's "Polanyian turn" or "soft centralization" of the early 2000s.[154]

When Xi Jinping took power, he initiated China's shift toward what Chiu-Wan Liu has theorized as recentralized authoritarian capitalism. There are many conceptual variations of re-centralization in China studies literature.[155] Xi marks a critical change in China's style of governance, according to Elizabeth Economy.[156] Other scholars argue that the strains of thinking

[154] Yang, "China's Illiberal Regulatory State in Comparative Perspective."; Andrew C. Mertha, "China's "soft" centralization: shifting Tiao/Kuai authority relations," Article, *China Quarterly* 184 (12/01 / 2005).
[155] For an extensive literature review of state capitalism versus authoritarian capitalism and decentralization/re-centralization, cf. Chiu-Wan Liu 2015, pp. 2-7.
[156] Elizabeth Economy, *The World According to China* (Wiley Publishers, 2021).

present in Xi were also present in his predecessors.[157] Both statements are true but are different in their form. Under Xi, the soft centralization has turned hard, and the leadership style has turned from relatively more consultative to personality-driven. Whereas before 2021, China's private sector was invited into the governing process, this changed abruptly after Jack Ma referred to China's banks as operating with a "pawnshop mentality" in a fall 2020 speech.[158] Meg Rithmire and Hao Chen have documented how China's mafia-like business systems both siphon off state assets and threaten CCP dominance.[159] Data regulation is one instrument through which the CCP can recapture control of economic outcomes and is consistent with Xi's hard turn.

On issues concerning civil society, China has preserved the human rights and dignitary aspect of the GDPR when it is exercised to control private sector overreach—particularly in areas such as predatory advertising or misappropriation of data. This is consistent with how China's government seeks to empower given elements of civil society as a feedback mechanism to improve governance. By allowing for a circumscribed range of citizen feedback, China can mitigate the classic "dictator's dilemma," which results when totalitarian regimes cannot make suitable policy choices because they lack accurate information about the real situation on the ground.

At the same time, there was also a hard turn evident in the PIPL. Whereas the CSL and earlier versions of the PIPL dating to 2019 hewed more closely to the GDPR in spirit, the later

[157] Yeling Tan, *Disaggregating China, Inc.* (Cornell University Press, 2022).
[158] "Jack Ma: Traditional banks are operating with a 'pawn shop' mentality," accessed 05/09/2022, https://www.thinkchina.sg/jack-ma-traditional-banks-are-operating-pawn-shop-mentality.
[159] Meg Rithmire and Hao Chen, "The Emergence of Mafia-like Business Systems in China," *The China Quarterly* 248, no. 1 (2021), https://doi.org/10.1017/S0305741021000576.

versions changed key features, such as consent, that materially weakened the power of the individual to control how their personally identifiable data is used. The final version was the most hardline, especially as it pertained to the general obligations of firms and data processors.[160]

Pearson argues that China has more than one political economy, and any analysis of China must consider this. Although there are many ways to cross-section China, the management of its private sector accounts for one of its political economies. Yang documents the growth of China's regulatory state and its Polanyian turn beginning in the early 2000s. Yang's work extends sequentially to Chiu-Wan Liu's proposed concept of "recentralized authoritarian capitalism" to describe how the failure of China's Polanyian turn to address the digital economy resulted in Xi Jinping's outright recentralization into an increasingly totalitarian model using the digital economy as the primary tool. In this sense, the PIPL is part of what Adam Tooze calls Beijing's "remarkable humbling of China's platform businesses, the second-largest cluster of big tech in the world…. The EU is a serious regulator but is nowhere near as menacing as Beijing."[161] This recentralization was first applied to the financial services sector after the GFC and was subsequently extended to the broader economy.

Previous authors who have compared the GDPR and China's emerging privacy laws have not looked at them in the context of the Brussels Effect, nor have they framed them in the broader China studies literature. Pernot-LePlay (2020) argues that China's initial attempts at data protection law run a middle ground between the EU and the US privacy standards, an

[160] *China's Personal Information Protection Law: A Comparison of the First Draft, Second Draft, and the Final Document*, (August 24, 2021), https://www.china-briefing.com/news/chinas-personal-information-protection-law-a-comparison-of-the-first-draft-the-second-draft-and-the-final-document/.
[161] Adam Tooze, "China under pressure, a debate," *Financial Times* (London) March 24, 2022.

argument that held until the draft PIPL. Building on Zoboff (2019), Aho and Duffield (2020) argue that whereas the EU's GDPR attempts to limit the power of what Zoboff calls "surveillance capitalism," China, by contrast, fully embraces the logic of surveillance capitalism to advance state interests. Geller (2020) argues that China's privacy regulations hew closely to the GDPR in important ways, most especially the adoption of concepts such as consumer consent to data collection, notification of consumers by firms about the nature and use of the data collected, and the consumer's right to have their sensitive information deleted when the purpose of the data use ceases to exist. These views are descriptively correct, highlighting different aspects of the law. Since these articles were published, however, the final version of the PIPL has been promulgated and therefore bears revisiting.

This chapter is organized as follows. It begins with contextual framing of the PIPL as part of China's overall legal system and cyber sovereignty framework. Second, the chapter reviews the sequencing of China's data governance framework. Third, it shows how the Brussels Effect explains China's reliance on the GDPR for data privacy regulation. Fourth, it explains that this regulation came to life in the context of a hard turn to a centralized and more ideologically-driven setting. This influenced the outcome of the final regulation. Finally, the chapter discussed how the final regulation helps the CCP fulfill its policy objectives.

4.2 Historical Context

The 21st century has been custom-made to highlight the Chinese Communist Party's (CCP) strength as an architect of narrative. In the Deng era through 1997, Western scholars and commentators pointed to China's manufacturing capacity, the strong work ethic of its people,

and its huge population as sources of its strength.[162] Above all, Deng was a pragmatist, and until the 1989 Tiananmen Square incident, he sought actively to solicit civil society input into China's governance.[163] Today's China is more about the CCP's capacity to structure narrative through centralized government control of massive economic platforms that gather, process, interpret and reinterpret data to suit its short- and long-term objectives. Its economic platforms include the Belt and Road Initiative, the Digital Silk Road, and its vast social media empires. Narratives competing with CCP orthodoxy vanish from the digital environment, sometimes abruptly but often softly as a light breeze. Alternatively, when competing for Western narratives like democratically elected governance and transparency cannot be eviscerated, those same powerful economic platforms can be used to redefine core concepts through rhetorical sleight of hand. Mao Zedong's essays are famous for shifting the logic midsentence to redirect attention away from inherent contradictions or unpalatable realities.[164] Thus, it is no accident that current Chinese President Xi Jinping has taken a page from Mao's example when in high-profile speeches, he seeks to redefine core Western values like democracy and human rights in terms of CCP preferences. A classic example of this has been China's attempt to reframe human rights in terms of the right to development.[165]

True to the Hegelian origins of Marxist thinking, Xi is leading China to a synthesis of Mao Zedong Thought with Deng's reform and opening to the outside world in the context of the

[162] Cf. writings by Barry Naughton and David Shambaugh, among others.
[163] Cf. Ezra Vogel, *Deng Xiaoping and the Transformation of China* (Cambridge: Belknap Press, Harvard University, 2011).
[164] Xing Lu, "The Rhetoric of Mao Zedong Transforming China and Its People," (University of South Carolina Press, 2017). https://muse.jhu.edu/book/51909/.
[165] The Right to Development: China's Philosophy, Practices and Contributions, (Beijing: People's Republic of China, 2016).

digital age. Xi's "dual circulation" strategy announced in 2021 may be the best current rhetorical example of this, even if the reality deviates from the rhetoric. The dual circulation strategy attempts to keep China engaged with the outside world, mainly as a consumer of its manufactured goods and social media services but aspires to insulate it from the vulnerability associated with overreliance on foreign technology and other inputs. Above all, it seeks to blunt the influence of Western values.

Like Mao and Deng, Xi is a transformative leader.[166] Xi follows Deng's footsteps in confirming his "'two hands' formula: a market-based economy and uncompromising political control."[167] In the "Explanation of the Chinese Communist Party Central Committee Decision on Several Major Questions About Deepening Reform", Xi emphasized that rule of law should be advanced under CCP leadership, in line with socialism with Chinese characteristics and with economic structural reform at the center of deepening reform. Deng could have penned these thoughts. However, in sharp contrast to Deng, Xi has reverted to the Maoist leadership style in important ways. For one, he pushed through an amendment to the CCP constitution at the 19th Party Congress, enshrining his thought as part of the Party's "guide for action." Deng would have abhorred such a move and eschewed efforts to enshrine his thinking in his lifetime. Moreover, Xi reversed the political tradition established by Deng, limiting the Chinese president's tenure to 10 years and implementing compulsory retirement at age 68 for Politburo

[166] Various schools of international relations argue about the relative importance of leaders, ideas, institutions, external factors, and other explanations for the course of historical events. For the purposes of this discussion, this chapter assumes that Xi Jinping is a driving force of China while acknowledging that no country or system is a monolith and many factors contribute to outcomes.

[167] John Garrick and Yan Chang Bennett, ""Xi Jinping Thought": Realisation of the Chinese Dream of National Rejuvenation?," Article, *China Perspectives*, no. 1/2 (2018).

members.[168] Xi turned 68 in 2021. When the CCP celebrated its 2021 centenary, Xi's leadership style was further cemented when the Party formally rewrote the canon of Communist Party history, softening the previous reinterpretation of Mao's leadership completed under Deng.[169] So, on the one hand, Xi is smashing long-held customs and norms established under Deng. On the other hand, he is simultaneously tightening his grip on power precisely by advancing Deng's agenda of establishing a strong legal system in what some have referred to as proto-Maoism.[170]

4.3 China's Legal System

Why is this the case? A strong regulatory framework, particularly around the digital economy, endows the CCP with the technocratic competence it lacked in the Mao era but reinstates the centralized control that was weakened during the Deng era. If securing economic growth is the key to the CCP's legitimacy, as Deng opined, and the digital economy is the ascendant driver of China's economic growth, then regulating the digital economy is the CCP's paramount mandate.

Xi's speeches often refer to what is translated from the Chinese as solidifying the "rule of law" (法治) but have in the West chiefly been interpreted as "rule by law." As Francis

[168] Garrick and Bennett, ""Xi Jinping Thought": Realisation of the Chinese Dream of National Rejuvenation?." Xi's retirement has been the subject of mammoth debate among Western scholars of China. Alice Miller provides useful insight into this discussion with the following: "…authoritative explanations for the abolition of the term limit on the post of PRC president imply that Xi's potential appointments beyond 2021–2022 do not convey an expectation of lifetime tenure. A long article in *People's Daily* on 1 March under the byline "Xuan Li"—a pseudonym for the party Propaganda Department's Theory Bureau—adhered to the standard line that the abolition of the term limit is "conducive to maintaining the stability" of China's unitary leadership system, by which the party general secretary serves concurrently as top military leader and head of state. But "Xuan Li" went on to note that the change does "not signify changing the retirement system for leading cadres of the party and the state, nor does it signify life tenure for offices of leading cadres.""

[169] Vogel, *Deng Xiaoping and the Transformation of China*.

[170] Guoguang Wu, "Continuous Purges: Xi's Control of the Public Security Apparatus and the Changing Dynamics of CCP Elite Politics," Minxin Pei ed. *China Leadership Monitor*, December 1, 2020, https://www.prcleader.org/wu.

Fukuyama has argued, in China "law was seen as a rational human instrument by which the state exercised its authority and maintained public order. This meant that … China has a *rule by law* rather than *rule of law*. The law did not limit or bind the sovereign himself, who was the ultimate source of law."[171]

Others have argued that today, China is best described by neither rule of law nor rule by law but as a "transitive" legal system. It is something between the rule of law and rule by law.[172] This claim is valid. The transitive model accounts for the fact that China's government agencies are constrained by the law just as they would be in a rule of law setting. This feature is present in China's PIPL, which holds government agencies accountable for protecting the data they collect and for collecting information legitimately. However, the CCP's lack of accountability to the law still makes it a rule by law regime. Like many Western conceptual frameworks, including rule of law and rule by law, they do not always capture the essence of what is at work in China. Hence, the need to understand China's internal logic on its terms.

Creemers argues that the most salient feature of the Chinese legal system today is that it is entirely new. "Few institutions or legal rules in their current form predate the beginning of the reform era. The People's Republic of China didn't require a Constitution to constitute itself."[173] Indeed, the impetus for reestablishing a legal framework under Deng was the drive for reform and opening up. The desire to encourage economic growth and a market economy led

[171] Francis Fukuyama, *Political Order and Political Decay: from the industrial revolution to the globalization of democracy* (New York: Farrar, Straus and Giroux, 2014). Pg. 357-358.
[172] Cf. Zhusheng Ye, "China's Transitive Legal System in the Reform Era: between Rule "by" Law and Rule "of" Law" (Ph.D., The Chinese University of Hong Kong (Hong Kong), 2014), https://www.proquest.com/dissertations-theses/chinas-transitive-legal-system-reform-era-between/docview/1674839768/se-2?accountid=11752 (3691981).
[173] Creemers, "Party Ideology and Chinese Law.", pg. 33.

to a proliferation of new laws regarding contracts, joint ventures, land use, and insurance, among others. These culminated in China's accession to the World Trade Organization (WTO). The sources of law were eclectic and piecemeal, serving the needs of the moment. This differed considerably, for example, from the Japanese legal reform, which made a whole-cloth adoption of the German code during the Meiji Reform of the 1890s.[174] In China, it was not until later that the ideological aspects of law came into relief, as pointed out by Creemers, who writes, "It took the Politburo until the 2000s to seriously consider the rule of law as something that might have a profound impact on state structuring and the relationship between state and citizen."

4.4 Regulation Sequencing

When Xi took power as general-secretary of the CCP in 2012, China lagged far behind other great powers in developing a cyber strategy. It was largely dependent on foreign IT software and operating systems and lacked a defense system against cyber-attacks on key infrastructure.[175] The Central Leading Group for Cyberspace Affairs was established in February 2014, with Xi appointed as the head. "Maintain cybersecurity" was first written in the Report on the Work of the Government during the National People's Congress and Chinese People's Political Consultative Conference.[176]

[174] Fukuyama, *Political Order and Political Decay: from the industrial revolution to the globalization of democracy*., pg. 365.
[175] Katherine Morton, "China's Global Governance Interactions," in *China and the World*, ed. David Shambaugh (Oxford: Oxford University Press, 2020).
[176] KPMG and China, *Overview of China's Cybersecurity Law* (2017), https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

Under Xi, China introduced the concept of "cyber-sovereignty" as an organizing principle of internet governance, in direct opposition to EU and US support for a global, open internet.[177] In Xi's words, cyber-sovereignty represents "the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing." [178] China's conception of cyber-sovereignty, as explained by Adam Segal, encompasses: 1) ensuring a "harmonious Internet," which implies government control of the narratives that appear on the internet and prevention of political agitation using social media; 2) reducing China's dependence on foreign suppliers of digital and communications equipment, and eventually leading the world in technologies such as AI, quantum computing, and robotics, and; 3) blunting the risk of cyberattacks on governmental and private networks that could disrupt critical services, curtail economic growth, or cause physical damage.

The harmonious internet concept referred at least partly to the rise of a vibrant online community of netizens, who had gradually become bolder in their public critique of the central and provincial governments. Before the rise of Weibo and WeChat, China's online community created internet influencers with many followers. Michael Anti was one of those online influencers, as documented by Elizabeth Economy in *The Third Revolution*.[179] He was well-liked for addressing sensitive political issues but was eventually (and ironically) censored by Facebook. It

[177] Future version of paper: possibly insert footnote explanation on the importance of "sovereignty" and "development" as two cornerstones of Chinese thinking since at least the Jiang era. Add citation from article by Chen Zhimin Fudan University.
[178] Segal, "When China Rules the Web."
[179] Economy, *The Third Revolution*.

is alleged that Facebook removed Anti because the company was still seeking to enter the Chinese market at that time.

The 2008 earthquake in Sichuan that killed some 87,000 people prompted massive citizen backlash online when the provincial government was slow to respond. Party cadres took notice and, fearing exposure of governing mistakes or embarrassing details of their private lives, they eagerly sought to curtail citizens' ability to post online without consequences. Nevertheless, subsequent attempts by the Hu Jintao administration to control the internet were limited. For example, self-regulatory conventions have advocated for real-name registration of online bloggers and other services. These largely failed, as the rapidly growing internet companies were reluctant to censor their users or delete accounts. At the same time, while Chinese government officials internally debated the dangers of free public discourse, different sections of its bureaucracy pursued diverging and often conflicting agendas.[180]

The inability of China's leaders to arrive at meaningful legislation on the internet is emblematic of why Xi rose to power and consolidated his rule. As Alice Miller has noted,

> *"In appointing Xi as general secretary, the party elite gave him enhanced authority so as to break policy deadlocks in the Politburo as well as new tools—such as the aggressive counter-corruption campaign and the concerted effort to centralize party power—to attack "vested interests" that had blunted progress in "double centenary" reforms deemed essential to the party's longer-term survival.*
>
> *The package of reforms pushed through the 19th Party Congress, and the 12th NPC seems to have doubled down on this approach. Xi's potential appointment beyond 2021–2022 is intimately intertwined with and conditioned on pursuit of the larger policy goals set down when he came to power. The broader political context of the abolition of the presidential term limit therefore amounts to an*

[180] Rogier Creemers, "The pivot in Chinese cybergovernance: integrating internet control in Xi JinpingÆs China," Article, *China Perspectives*, no. 4 (01/01 / 2015).

acknowledgment that the old CCP adage "only socialism can save China" requires the new corollary that "only Xi Jinping can save socialism."[181]

From this view, regulating the digital economy is central to saving socialism. The first major piece of legislation in this effort was the Cybersecurity Law of 2016 (CSL). The CSL is the fundamental law regulating cyberspace, covering personal information and "important data." According to Hong Yanqing, an early drafter of the PIPL, the CSL did not provide "systematic thinking, let alone comprehensive institutional designs" to effectively protect data and data rights.[182] The Data Security Law (DSL) and the Personal Information Protection Law (PIPL) were passed in June and August 2021, respectively. Collectively, the CSL, the DSL, and the PIPL comprise China's complete legal data governance regime.

Unlike the GDPR, China conceptually segregated data protection and data privacy. The DSL is the fundamental law regulating data security, establishing a framework for data protection against cyber threats writ large, including non-personal information. The PIPL, by contrast, marks the introduction of a comprehensive system for the privacy and protection of personal information. It provides details for administering the requirements outlined in the CSL and narrows key definitions, such as what constitutes a data subject's consent to having his/her data processed. It also seeks to operationalize the right to privacy established by China's 2020 *Civil Code* (Article 1032), in which privacy is defined as "the undisturbed private life of a natural person and his private space, private activities, and private information that he does not want to be known to others."[183] The Civil Code of 2020 goes on to outline what is meant by undisturbed

[181] Alice Miller, "Only Socialism Can Save China; Only Xi Jinping Can Save Socialism," Article, *China Leadership Monitor* 56 (Spring2018 2018).
[182] Hong Yanqing, quoted in Creemers 2021. Creemers, "China's Emerging Data Protection Framework."
[183] Civil Code of the People's Republic of China, (Beijing: People's Republic of China, 2020).

private life. It includes a prohibition on intruding on people's private life with phone calls, text messages, instant messages, and flyers; taking pictures of people's private spaces, private activities or body parts; eavesdropping, and; processing private information without consent. It also includes a provision to prohibit sharing private information that subjects "do not want to be known" (Article 1032).

The late arrival of the PIPL legislation relative to the CSL is evidence of an evolutionary process through which the Chinese state came to understand the rich interaction between regulatory enforcement and engaging citizens who could aid in the process of calling attention to private sector infringements if offered legal avenues, such as redress through the courts. In the interim between the CSL and the PIPL, many data protection administrative rules, guidelines, and cybersecurity reviews were rolled out. Many of these were market-regulating measures similar to those taken in the European Union under the Digital Markets Act and the Digital Services Act. For example, in March 2022, the Cybersecurity Administration of China (CAC) introduced legislative provisions on the scope of necessary personal information for common types of internet applications. These provisions prohibit application providers from refusing users access to essential functions if they do not provide additional personal information beyond necessary personal information.[184]

4.5 China and the Brussels Effect

What motivated China to consider the EU's data privacy regulation? China's adoption of GDPR-like rules was both voluntary and independent of China's relationship with the EU.

[184] Ping West, "Timeline: China's Tech Crackdown 2021," Ping West ed. *China Tech Last Week*, August 31, 2021, 2021, https://pingwest.substack.com/p/timeline-chinas-tech-crackdown-2021?s=r.

Chinese domestic issues played an important role, as did China's ongoing ambition to establish the regulatory framework of a modern nation. Outside influence from the European Union was of scant importance.

In the 2000s, there were early attempts to introduce legislation on data protection in China. These efforts were thwarted by jockeying among competing Chinese government institutions.[185] Not until internet access burgeoned and Smartphones entered the market did data privacy become a more salient issue, prompting greater regulatory action. When it did, it was entirely consistent with the Deng era for the authors of the DSL and the PIPL to build on the practice of adopting laws from eclectic sources.

4.5.1 Process-Tracing the PIPL in China

In 2016, China established the Personal Information Protection Specification task force headed by Hong Yanqing, who looked to privacy guidelines published by the OECD, the EU, and the California Consumer Privacy Act. Hong studied human rights law in his PhD program in the Netherlands and was deeply familiar with the European legal system. According to MIT's Karen Hao, China was prompted to undertake a thorough revision of individual data privacy regulations directly responding to two events. First, the GDPR made Chinese regulators recognize that firms with an international footprint or aspirations would need to understand and comply with the law. They responded not just to the need for Chinese businesses to comply with EU regulations where they operated but also to the extraterritorial feature of the GDPR. Second, a 2016 Internet Society of China survey found that 84% of respondents had suffered some form of

[185] Creemers, "China's Emerging Data Protection Framework."

personal data loss. This led authorities to worry that consumers would become reluctant to participate in the digital economy.[186]

Hong Yanqing noted that the review of all the global privacy regulations ultimately came down to a debate between the US and European models. When Hong's task force released its first data privacy guidelines, the Personal Information Privacy Standard (PIPS), in May 2018, they followed the EU in adopting its more stringent standards, but they followed the US in making the standards voluntary and non-binding. They took the middle road between the EU and the US. All that changed with the Cambridge Analytica scandal when regulators decided data privacy regulation needed more teeth. The onset of COVID hastened the process of tightening rules as a result of public outcry over aggressive health data collection by local authorities. This outcry ultimately prompted the National People's Congress to announce that they would fast-track the work of passing the PIPL. The European model had prevailed with its strict standards and supervisory requirements.

4.5.2 EU Lobbying?

Direct external influences appear to have played a minor role in how China arrived at its legal framework for the digital economy. Comprehensive EU-China contacts on cybersecurity and data privacy have been sparse. The EU and China did not hold high-level talks on data protection until September 2020, at which point China had already drafted its initial privacy law and was engaged in consultations with Chinese academics and practicing lawyers on the topic. Prior to that, informal consultations included the annual Information and Communication

[186] Karen Hao, "Inside China's unexpected quest to protect data privacy," *MIT Technology Review* (August 19, 2020 2020). https://www.technologyreview.com/2020/08/19/1006441/china-data-privacy-hong-yanqing-gdpr/.

Technologies (ICT) Dialogue with China at a technical level, covering ICT and digital policies as well as regulatory issues, started in 2009. In addition, the European External Action Service and the European Commission co-chaired an EU-China Cyber Taskforce founded in 2012. This latter forum has a mandate limited to "enhancing exchanges on cyber issues."[187]

Beyond the EU, its member nations' bilateral relations with China also saw only a narrow dialogue on cybersecurity. The signature issue that focused EU-member governments' attention was the adoption of Huawei technology in the context of bilateral trade negotiations. For Huawei, the results initially were split. Both the UK and Sweden banned Huawei telecommunications products in their countries.[188] Under German Chancellor Merkel's leadership, Germany had long taken an accommodative stance toward Huawei largely because of strong German car sales to China. Germany sells more cars to China than any other country besides the US.[189] In this case, it was not Germany influencing China but the other way around. Today, German telecom suppliers have long-standing partnerships with Huawei and decades' worth of its equipment in their existing networks. Any replacement will be extremely costly. In its draft IT security law, Berlin offered a bureaucratic solution to the vendor security issue without explicitly banning Huawei equipment.[190] One might be tempted to refer to the effective influence on

[187] "EU-China: Commission and China hold first High-level Digital Dialogue," news release, September 10, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1600.
[188] Beryl Thomas, "What Germany's new cyber security law means for Huawei, Europe, and NATO," (02/05/2021 2021). https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/.
[189] "Leading import countries for motor vehicles from Germany in 2021, by value of exports," Statista, accessed September 26, 2021, https://www.statista.com/statistics/587701/leading-import-countries-german-motor-vehicles-by-export-value/.
[190] Germany's draft IT Security Law 2.0 evaded the issue of vendor security. The legislation has been harshly criticized for its complicated two-part assessment mechanism for telecom vendors seeking access to Germany's 5G networks. Along with a technical evaluation, the draft law requires a vendor to issue a declaration that its components cannot be used for "sabotage or espionage". The law only allows for the exclusion of a vendor if all involved authorities are unanimous in their decision to enact a ban. See Stefan Krempl, "IT-Sicherheitsgesetz 2.0:

Germany's Huawei position as a "Beijing Effect." COVID, however, created a different mood in Germany. Ultimately, it fell closer into line with the rest of the EU. The IT Security Law 2.0 approved by the Bundestag restricts the role of "untrustworthy" suppliers of 5G technology and requires telecom operators to notify the government if they sign contracts for critical 5G components. It also gives the government powers to block them.[191]

In sum, China's adoption of GDPR rules seems to have occurred quite independently of Brussels, despite the challenges Huawei faced in the EU market. So how did the GDPR fit into the internal logic of China's political economy such that it could be adopted without external influence from the EU? This is the topic of the next section.

4.6 The Logic of Regulating the Digital Economy: Hayek to Polanyi to Recentralized Authoritarian Capitalism?

Remembering the opening anecdotes from Nicholas Kristof in Chapter I of this thesis, the late 1980s and early 1990s in China were the beginnings of a free-wheeling era of business entrepreneurship. The Cold War had ended, China and the United States were on better terms, and Deng's pragmatism led to the massive influx of foreign technology into China.

Internationally, US global dominance led to the embrace of liberal markets as embodied in the proliferation of trade agreements (NAFTA, GATT, and WTO) and the attendant explosion of global trade. In the early 1980s and 1990s, this trade was heavily focused on trade in goods,

"Mittelfinger ins Gesicht der Zivilgesellschaft" " (December 10, 2020). https://www.heise.de/news/IT-Sicherheitsgesetz-2-0-Mittelfinger-ins-Gesicht-der-Zivilgesellschaft-4986032.html. See also Patrick Beuth, "Das soll im Huawei-Gesetz stehen," *Der Spiegel* (December 12, 2020). https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-2-0-das-soll-im-huawei-gesetz-stehen-a-169932f8-94ab-42c2-903f-0fc84fb5fb93.

[191] Gesetz zur Erhöhung der IT-Sicherheit mit Koali-tions-mehrheit beschlossen, (Deutscher Bundestag (German national parliament), 2021). Deutscher Bundestag - Gesetz zur Erhöhung der IT-Sicherheit mit Koalitionsmehrheit beschlossen

in which China developed a strong comparative advantage. For its part, the European Economic Community began an intensive new stage of economic integration with the conclusion of the 1992 Maastricht Treaty, which set the continent on the path toward a single currency. This single market integration involved the development of a far deeper and wider regulatory body than had previously existed. That same year, Deng Xiaoping took his famous Southern Tour of China in which he famously said, "to get rich is glorious."[192] The EU and China both had much to gain by embracing the Anglo-American approach to economics, and to a significant degree, they did so. Dali Yang refers to China's Hayekian turn in the late 80's and early 90's as its economic and social equivalent of a "Cambrian explosion." [193] As the Chinese economy became more globalized, the government-initiated waves of reform to rationalize its governing structure and adjust it to reflect China's new economic model.

Nevertheless, despite the embrace of free markets, it was in fact the beginning of a great regulatory expansion around the globe. Since US President Ronald Reagan and UK Prime Minister Margaret Thatcher, independent regulatory bodies have proliferated despite the prevailing narrative that announced the demise of government.[194] Freer markets do not function on their own. Deregulation was accompanied by the creation of more rules and rule-making institutions, as argued by Vogel.[195]

---

[192] https://store.hbr.org/product/china-to-get-rich-is-glorious/707022?sku=707022-PDF-ENG

[193] Yang, "China's Illiberal Regulatory State in Comparative Perspective." Karl Polanyi's economic classic is his 1944 book, *The Great Transformation,* which posits that markets are political and therefore should be subject to political control. Polanyi's "opposite" would be Friedrich Hayek, who believed that the markets should be free and essentially left to their own devices. Both were contemporaries living in Vienna at the time of the Bretton Woods conference.

[194] See, for example, Martin van Creveld, *The Rise and Decline of the State* (Cambridge: Cambridge University Press, 1999).

[195] Steven Kent. Vogel, "Freer markets, more rules : regulatory reform in advanced industrial countries," (Ithaca :: Cornell University Press, 1996).

In Europe, the proliferation of the Brussels bureaucracy dominated by regulatory experts independent of political accountability to voters regularly invited critics to lament the EU's "democratic deficit."[196] Borrowing from a conceptualization by Matthijs and Parsons:

> "The EU is a polity that pursues Hayekian normative goals (of cross-border openness and market discipline) in ways that fit Polanyian analytical expectations (which theorize that such openness requires strong central authority).... The result resembles the thinking of German ordo-liberals, who share Hayekian goals but envision stronger central authority to enforce it.... Today's EU displays even more extensive and active central authority than ordo-liberals have advised. The Polanyian muscles in this Hayekian Brussels amount to a kind of ordo-liberalism on steroids."[197]

Nothing could seem more natural to Chinese leaders than a Polanyian turn in support of a Deng's "socialist market economy." In China, this development was seen as a sign of modernization. It represented the professionalization of governance, an ideal Weberian bureaucracy insulated from the vicissitudes of public clamor.[198] Throughout the 1990s and 2000s, as Dali Yang notes, "China's leaders reconstituted the sinews of governance and especially sought to strengthen the government's regulatory capacity while reducing the government's direct intervention in state firms. In area after area, they have invoked "chaos" or "turmoil" to justify the need to strengthen or assert control."[199] Polanyian governance was the solution to the perception of looming chaos while allowing for strong economic development based on market forces.

The Global Financial Crisis (GFC) changed all that. It prompted a shift in China's Polanyian style of market-dominated governance; authority became more centralized yet, and more

---

[196] See, for example, Petr Kratochvil, "The end of democracy in the EU? The Eurozone Crisis and the EU's Democratic Deficit," *Journal of European Integration* Vol. 41 Issue 2 (2019).
[197] Matthias Matthijs and Craig Parsons, Muscles in Brussels: The European Union's Economic Authority in Comparative and Theoretical Perspective, 2019. Unpublished draft paper.
[198] Max Weber, *From Max Weber: Essays in Sociology* (New York: Oxford Press, 1946).
[199] Yang, "China's Illiberal Regulatory State in Comparative Perspective.", pp. 119.

importantly, the role of the market economy was demoted. By taking a strong and decisive central government approach to the crisis, China's government averted much of the economic fallout that the rest of the world suffered. China's success in confronting the crisis not only enabled its spectacular economic growth to continue but also gave Chinese leaders an unprecedented sense of self-confidence. Finally, it also precipitated a profound disillusionment about the United States and liberal economic models. To many in China, the country's stronger performance during the crisis vindicated its choice of development model.

Barry Naughton shows evidence of a decisive change in a Government Working Report presented by Chinese Premier Wen Jiabao. This report recalibrated the previous CCP emphasis on market forces and again elevated central control ("macro-control") to the same level as market forces. By putting central control rhetorically on par with the market economy, this report, in classic Chinese style, quietly ushered in an era of greater centralization and economic rebalancing that would be extended beyond monetary and fiscal policy to all areas of government. As Naughton notes, Wen Jiabao's Working Group document "was probably the most unambiguous movement to reemphasize centralization and use of administrative instruments to govern the economy since the term "socialist market economy" was incorporated into official Chinese rhetoric in September 1992."[200] Naughton cites changes in China's monetary policy, housing, technology, energy, and healthcare sectors. The GFC indeed caused a tectonic shift in China's style of governance.

[200] Naughton, "China's Response to the Global Crisis, and the Lessons Learned." Pp. 24.

However, as documented by Rogier Creemers, the same centralization impulse was notably absent from the digital sector.[201] This is partly because big data, cloud computing, and the internet of things had not yet emerged as major issues.[202] As early as 2003, China's top entrepreneurs had been invited into the internet governing process.[203] Alibaba's Jack Ma, Tencent's Pony Ma, and Baidu's Robin Li were invited to join as vice directors of the Internet Society of China, a consultative organization under CCP guidance. Some were also invited to join the 3,000-member People's Congress of China, the body that rubber-stamps new policies set forth by the Politburo. These entrepreneurs actively lobbied against stricter controls on how private sector companies use data and were successful in the early years.[204]

It was not until Xi Jinping that China established the sinews of governance for its digital economy. The emergence of the internet and the GFC together contributed to a recognition that unleashing market forces in China had the dangerous consequence of introducing greater social instability. Recognizing that technology had advanced more quickly than the government's ability to control it, Chinese President Hu Jintao moved more rapidly in the early 2010s to construct a policy. However, it was not until Xi that a regulatory framework spanning cybersecurity, the digital economy, and online media content emerged under one mantel.[205]

---

[201] Creemers, "China's Emerging Data Protection Framework.", pp. 7.
[202] Yehan Huang and Mingli Shi, "Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law," (June 8, 2021). https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/.
[203] "China's once-shunned entrepreneurs join Communist Party," (October 6, 2007). https://www.spacedaily.com/reports/Chinas_once-shunned_entrepreneurs_join_Communist_Party_999.html.
[204] Fu, "China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent."
[205] See, for example, Elizabeth Economy for a discussion of measures taken before Xi Jinping. Economy, *The Third Revolution*.

4.7 Similarities between the PIPL & the GDPR

Central government regulation of the data economy achieves the following policy goals: 1) rebalances the central government's relationship with the private sector by creating mechanisms for compelled government access to data that would open the kimono to government officials to have better insight into the functioning of private firms; 2) demonstrates government responsiveness to citizen complaints about unfettered private sector data gathering; 3) increases the surveillance capacity of the government writ large, allowing for the creation of monitoring mechanisms, such as the social credit system, and; 4) indirectly addresses China's long-standing problem of fragmented authoritarianism under which provincial or local implementation of central directives was often ignored or actively undermined by officials (data collection as a tool of accountability) and allows the local government to improve the delivery of social services.

The next section discusses each policy implication in turn and shows the PIPL features designed to advance these policy objectives.

4.7.1 Extraterritoriality

Like the GDPR, China invokes extraterritoriality in its data privacy law, limiting the flow of Chinese citizen data outside its borders. In its current form, the requirements for data localization are almost total. The law specifies that firms holding data for a given threshold of individuals, a number that has yet to be published, must keep the data within China unless they obtain a security review with the Cybersecurity Administration of China. Given the imprecise nature of the law, this amounts to complete data localization for any firms doing business with China. While the extent of data localization in the EU is limited to those entities that do not make use

of the data transfer instruments that conform to the *Charter of Fundamental Rights* (see Appendix 2), China's data localization objectives are entirely separate from the desire to protect the human rights of its citizens. Instead, it is loosely related to Xi's articulation of cyber sovereignty, through which China hopes to minimize its perceived vulnerability to Western technology. While the Great Firewall of China limits the inflow of information into China, the PIPL limits the outflow of personally identifiable information about Chinese citizens.

4.7.2 Individual Rights

The PIPL provides comprehensive measures that were more vaguely represented in the CSL when it passed in 2016, as previously mentioned. Looking at the PIPL through the specific definition of the Brussels Effect—the transmission of regulatory policy without coercion or cooperation—the GDPR's influence is clear. Moreover, within the context of commercial transactions, the human rights/dignitary aspects of the GDPR are preserved and indeed protected more vigorously than even in the United States. This may be surprising to a casual observer, given the current Western narrative about the CCP and Xi Jinping, but is entirely consistent with the broader picture in China. Data subjects have significant control over their commercially-held data and have the right to seek redress in the Chinese courts. The individual right to redress has been a point of contention between the EU and the US, where court cases against corporate violations of data protection can only be brought by regulators, such as the FTC under the Federal Trade Commission Act.[206] US persons do not have the right to pursue remedy except in the cases of defamation of character. Table 2 shows the degree to which the PIPL matches the GDPR:

[206] Article 5 of the act empowers the FTC to root out "unfair or deceptive acts or practices."

TABLE 2: GDPR VS PIPL RIGHTS AND BUSINESS OBLIGATIONS

Rights under the GDPR	Rights under the PIPL
Right to information	√
Right to access	√
Right to correction/rectification	√
Right to erasure	√
Right to object to and restrict the processing of an individual's data	√
Right to data portability	√ (but needs to satisfy conditions stipulated by the Cyberspace Administration of China)
Right not to be subject to automated decision-making	√
Right to withdraw consent	√
Right to lodge a complaint with the regulator (private right of action/redress)	√

Business Obligations under the GDPR	Business Obligations under the PIPL
Opt-in default (requirement age)	×
Notice/transparency requirement	**limited**
Risk assessments	√
Prohibition on discrimination (exercising rights)	√
Purpose/processing limitation	√

source: IAPP

The table above shows that the PIPL checks all the GDPR boxes. Like the GDPR, the PIPL requires personal information handlers to ensure that personal data is processed for a clear and reasonable purpose, it must be transparent, and data may be retained only for the minimum time needed to achieve the purpose of the processing. The relationship between processors

and third-party handlers are governed by conditions set out in the PIPL that are very similar to GDPR requirements on data processing agreements between data controllers and processors.

Both the PIPL and the GDPR create mechanisms for the protection of data subjects' rights and interests, including detailed rules on informed, voluntary, and clear consent, the right to withdraw consent, automated decision-making (e.g., credit evaluation), and transparency of processing (e.g., a requirement to notify data subjects of the identity of the entities handling their information, where that information is transferred, and what information is processed). They prohibit firms from making data subject consent a condition of receiving a service. Like the GDPR, the PIPL also requires corporations to ensure the confidentiality and security of personal data, including conducting security and impact assessments and procedures for handling personal data breaches.[207]

In its final form, the PIPL links data privacy to its anti-trust drive, which was targeted specifically at China's mammoth tech sector. While the *right to data portability* did not exist in prior versions of the PIPL, the final version draws closer to the GDPR by granting individuals the new right to extract their data from one platform or service and store or use it elsewhere. Article 45 requires that personal information handlers comply with people's requests to transfer their data to another handler if the transfer meets conditions yet to be set by the CAC. The rules have not yet been fleshed out. This addition reflects China's response to internet platforms that have leveraged large troves of user data to lock users into their platform ecosystem and fend off emerging competitors. It is widely held that increasing data portability will

[207] "Analysis of China's Draft Personal Information Protection Law," Arnold & Porter, 2020, https://www.arnoldporter.com/en/perspectives/publications/2020/11/analysis-of-chinas-draft-pip-law.

enhance market competition, benefitting consumers and fueling innovation. A Chinese anti-trust guideline published in 2021 considers data-related switching costs to users in assessing market entry barriers and finds that data portability will benefit consumers.[208] In practice, this is easier said than done, as EU regulators have learned over the short history of the GDPR.

Finally, like the GDPR, the PIPL standards are explicitly written to apply to government entities—partly in response to the public outcry over local authorities' perceived overreach on data collection during the COVID pandemic. As such, China's privacy law purports to constrain, as well as empower, public authorities. Without the individual's consent, state organs must not publicly disclose or provide others—including other state organs—with personal information they handle absent authorization stipulated in law (Article 36). State organs must further comply with general requirements relating to automated decision-making (Article 25) and facial recognition and surveillance for public safety purposes (Article 27). This summarizes the protections for individuals and their similarities to the GDPR. Despite these similarities, a wide array of derogations unsurprisingly undermines the protection of individuals from state intrusion. These derogations reflect China's broader policy objectives under Xi Jingping.

4.8 Differences from the GDPR & the policy implications

Centralized control of national, subnational, and firm-level data directly addresses Xi Jinping's express goal to mitigate domestic contradictions that had arisen from the Deng era

[208] "Guidelines of the Anti-monopoly Commission of the State Council for Anti-monopoly in the Platform Economy (国务院反垄断委员会关于平台经济领域的反垄断指南（2021 年 2 月 7 日国务院反垄断委员会印发）)," Government of the People's Republic of China accessed March 10, 2021, https://gkml.samr.gov.cn/nsjg/fldj/202102/t20210207_325967.html.

and is directed at three constituencies: firms, local and provincial governments, and citizens. The PIPL is directed at these groups in different ways.

4.8.1 Rebalancing the Private Sector-State Relationship

As we saw in an earlier section, government officials appeared to have started consultations on data privacy legislation both in response to the global ambitions of Chinese firms and as a means of shoring up consumer confidence in the digital economy. The various drafts of the law provide evidence of an evolutionary process through which it gradually evolved into a more punitive and restrictive instrument targeted at what the government perceived as insubordinate Chinese mega-firms.

Outside of China, much has been written about how China's entrepreneurial and management elites have benefited from the government promotion of national champions and have been coopted by the CCP. There is unquestionable alignment between the state and firms at given intersections. For example, the innovative capacity of private technology firms in fintech and AI makes them both valuable to the economy and facilitates CCP legitimacy. It also makes the government a potential customer of their technologies and services. As central, provincial, and local government entities seek to digitize their citizen services, they have become the largest consumers of China's cloud service providers. Finally, tech manufacturers like Huawei benefit from spreading Chinese hardware and other home-grown technologies through the Digital Silk Road. Thus, it would be no surprise that—once China formally allowed private sector entrepreneurs to join the Communist Party—Pony Ma, CEO of Tencent, and Jack Ma, retired CEO of Alibaba, were invited to join. They were subsequently granted seats in the National People's Congress and were invited as members of the prestigious Internet Society of China.

Nevertheless, until the recent tech crackdown, reporting outside of China about the degree to which these firms have challenged the government has been relatively sparse. One example of such a challenge is a 2018 clash between the Chinese ride-sharing company Didi, and regulators over real-time access to its data illustrate the point. After the murder of two passengers, Didi resisted turning over data to law enforcement investigators, using customer privacy to justify their stance. Didi finally relinquished the data to Wenzhou police after two rejections, including one attempt to hand over data printed on paper in non-standard, essentially unusable form.

The tug-of-war between the government and companies over data illustrates a larger point. Besides the government, the BATs and JD.com are the three largest aggregators of data in China.[209] The information that these companies gather not only makes them potent drivers of economic growth in China, it also gives them leverage. Rithmire and Chen document the emergence of Mafia-like business systems in China that would have led government officials increasingly to perceive the massive Chinese platforms as a threat rather than merely as a partner.[210] When Jack Ma made a speech in 2020 accusing government regulators as "operating with a pawnshop mentality," it sparked a fierce backlash that resulted in the IPO cancellation of Alibaba's $38bn subsidiary, Ant Financial.[211] It also led to a broader tech crackdown that has been widely covered in the media, many of them framed as anti-trust violations.[212] The addition

[209] Jason Ding, *China Internet Report* (March 26, 2021), https://www.bain.com/insights/china-internet-report/.
[210] Rithmire and Chen, "The Emergence of Mafia-like Business Systems in China."
[211]"How billionaire Jack Ma fell to earth and took Ant's mega IPO with him," Reuters, updated November 5, 2020, https://www.reuters.com/article/ant-group-ipo-suspension-regulators/how-billionaire-jack-ma-fell-to-earth-and-took-ants-mega-ipo-with-him-idUSKBN27L2GX.
[212] Jill Disis, "China fines Alibaba, Tencent and Baidu for more antitrust violations," (November 22, 2021). https://www.cnn.com/2021/11/22/tech/alibaba-tencent-fines-intl-hnk/index.html.

of *data portability* to the final version of the PIPL was one piece of the broader tech crackdown of 2021. Moreover, to show tech entrepreneurs that the CCP meant business, the government legislated a maximum fine for PIPL violations of 5% of global revenues versus the GDPR's 2%.

The adoption of data privacy regulations alters the balance of power between the Chinese state and foreign and domestic private sector firms, chiefly Alibaba, Baidu, and Tencent, who have gathered vast amounts of consumer data. This data is housed internally, creating a significant competitive advantage for Chinese firms. These regulations grew out of China's centralization of fintech regulation after the GFC. Like the EU, China reacted to the GFC by imposing new measures to shore up systemic fragility. In the EU, the regulation of the fintech sector preceded data privacy regulation, although they were closely intertwined, as shown in Appendix 3.

4.8.2 Citizen Agency as a tool of Authoritarian Optimization

The second policy consequence of the PIPL is that, even as the government increases its citizen surveillance, its adoption demonstrates government responsiveness to increased civil society awareness of data privacy and fraud related to data theft. The notification and consent specifications adopted from the GDPR are signs of this responsiveness, even in their curtailed form. (The limits on consent are discussed in the context of surveillance in the next section.) Such regulation might be understood as a form of satisficing – a term coined by economist Herbert Simon—rather than maximizing authoritarian rule.213 By satisficing, citizens feel that the government acts meaningfully in response to perceived injustice and gain a sense of agency

[213] Fukuyama, "The Origins of Political Order." Pgs. 471-472. Fukuyama discusses Herbert Simon's concept in the context of Chinese emperors and their tax collection practices. However, there is application in the data governance sphere as well.

that is often demotivating in a completely totalitarian setting. China's government does indeed inspire citizen confidence in its leadership, as was shown by an Ash Center survey.[214] In addition, citizens can then act as enforcement agents by bringing cases that draw attention to violators. Redress, if indeed enforced by the courts as they have been recently, can be a powerful legitimator of CCP rule.

Data privacy has become an exceedingly hot topic in China because of the vast numbers of identity theft, fraud, and other events that have prompted public outcry.[215] One month after the first Draft PIPL was published, a ruling in the trial of a highly publicized case was touted as the "first lawsuit against facial recognition." The victory of the plaintiff, a law professor who had objected to the use of the technology by the Hangzhou Safari Park, generated a flurry of domestic news coverage and social media chatter.[216] Facial recognition is a technology of particular concern to Chinese citizens, as it is adopted in security surveillance systems in airports and other places and increasingly in financial and banking systems for ID verification and mobile payment. The Hangzhou Safari Park lawsuit galvanized immense public attention in China and highlighted the lack of regulation in the adoption of facial recognition.

In addition to the highly visible case of the law professor and the Hangzhou Safari Park, individual consumers have also brought cases against big tech companies. In Ling vs Douyin/Duoshan, when registering for the two social apps, the plaintiff Ling was prompted with a list of

[214] Cf. Cunningham, Saich, and Turiel, *Understanding CCP Resilience: Surveying Chinese Public Opinion Through Time*.
[215] There is vast media coverage of Chinese consumers' concern for their data privacy. See, for example, Winston Ma, "China is waking up to data protection and privacy. Here's why that matters," (11/12/2019). https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline/.
[216] Xiao Liu, "Understanding China's Governance Space around Personal Data," in *Essays on the Rise of China and its Implications*, ed. Abraham M. Denmark and Lucas Myers (Washington, D.C.: Wilson Center, 2021).

"people you might know" on the apps. Suspecting the app had read his phone contacts list without consent, he sued the app provider, Bytedance. In a separate case, Huang vs Tencent, the plaintiff Huang, in using the app WeChat Reading, found her reading information was shared with her "friends circle" in the WeChat app without her knowledge. Huang brought the case against the parent company of the two apps. Although the issues these citizens litigated against what seemed to be minor in the sense that "no actual harm" could be proved, their "low-stake" nature highlighted the symbolic significance of the lawsuits. In short, government responsiveness to civil complaints regarding firm overreach in the use of personal data lends agency to citizens and credibility to the regulatory efforts, even as they are used against individual citizens by the government.

4.8.3 Governance, Surveillance and the Nascent Social Credit System

Third, we return to the power lost by the *danwei* (单位) when China's reform and opening up eviscerated the dominance of the once all-important *dang'an (档案)* that started this thesis in Chapter I. The social credit system (SCS) has emerged as a mechanism to recapture some of the social control forfeited by the government when Chinese citizens became free agents in the workforce. Nevertheless, as with many initiatives in China, the SCS has grown far beyond its initial conceptualization. In its earliest form, the government in 1999 under Premier Zhu Rongji conceived a plan to alleviate foreign firms' challenges in obtaining information on their Chinese partners.[217] The SCS became an integral part of the effort by the CCP to create a "unified, open, competitive and orderly modern market system." It was discussed in official

[217] Eunsun Cho, "The Social Credit System: Not just another Chinese Idiosyncracy," *Journal of Public and International Affairs* (2020), https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy.

documents only in the context of market reforms.[218] In 2007, credit, tax, and contract performance records were suggested as potential elements of one's social credit status, not unlike credit scores in the United States.[219] By 2014, the government sought to formalize and coordinate efforts around the SCS. They released a plan that would extend financial credit scoring systems to other areas of government regulation, from contract enforcement to food safety, corruption, and environmental protection.

While still under construction, the SCS is meant to link public and private data on financial and social behavior across China, use the data to evaluate the behavior of individuals and organizations, and punish or reward them according to certain agreed upon standards of appropriate conduct. While many SCS goals are laudable, the scale and potential impact pose serious risks to individuals and organizations that could result in the opposite of the promised effects. By gathering ever more centralized data, the government can both improve the delivery of government services and to exercise greater social control over individuals. Yet, the reality is that the social credit system is still weakly interconnected and evenly more poorly understood.

After generations of purges under Mao and anti-corruption campaigns in the reform era, China is a low-trust society quite different from the West. As a result, the idea of a social credit system is popular with citizens.[220] The narrative that the social credit score can build trust in the digital economy provides a veneer of legitimacy to secure individual compliance. The

[218] Zemin Jiang, Report at 16th Party Congress on Nov 8, 2002, (Beijing: Ministry of Foreign Affairs of the Republic of China, 2002).
[219] Martin Chorzempa, Paul Triolo, and Samm Sacks, *China's Social Credit System: A Mark of Progress or a Threat to Privacy?* (June 2018), https://www.piie.com/publications/policy-briefs/chinas-social-credit-system-mark-progress-or-threat-privacy.
[220] Genia Kostka, "China's social credit systems are highly popular – for now," (September 17, 2018). https://merics.org/en/analysis/chinas-social-credit-systems-are-highly-popular-now.

notification and consent features of the PIPL provide this veneer, although not without some genuine benefits to individuals.

The consent requirement falls under the broader European legal concept of *legal basis* within the GDPR. Consent is one of six legal bases for collecting and processing an individual's data, including the necessity to fulfill an existing contract; for public health crisis (COVID), among others. These are more generally defined in the GDPR but complemented by other laws constraining the potential for government abuse. Notification requirements reflect a separate legal category, but the concepts of notification and consent are often linked in the discussion of data and human rights protections.

Requirements for notification and consent evolved throughout the legislation's debate, which produced two drafts and a final version. From the first draft to the final version, both sets of requirements were refined to give greater discretion and privilege to data gathering entities and fewer protections for individuals, with one exception. That exception was the data portability requirement discussed in connection with cracking down on China's big tech firms.

Under the Cybersecurity Law of 2016, explicit consent was the only lawful basis for collecting and processing personal information.[221] Thus, the CSL at least technically protected the individual more than the GDPR because it did not include the other legal bases for data collection that the GDPR did. The first draft of the PIPL, released in October 2020, incorporated all the collection and processing requirements of the GDPR. The final version added yet another

[221] Articles 22, 41, and 42. Rogier Creemers, Graham Webster, and Paul Triolo, Cybersecurity Law of the People's Republic of China (Translation), (Stanford: Stanford University Digichina, 2018).

provision that weakened privacy by allowing for the processing of publicly available data or "personal information disclosed by the individual themselves." (Article 13)

Notification provisions significantly narrow individual protections under the banner of state secrecy. State secrecy provisions are not present in the GDPR. The state secrecy provisions are the obvious loophole that opens the door for government surveillance. For example, Article 19 states that information handlers "*are permitted not to notify individuals*…under circumstances where laws or administrative regulations provide that secrecy shall be preserved or notification is not necessary." (*italics = author emphasis*) This leaves enough room in the law to allow for a great deal of state discretion over whether individuals are made aware of information that is shared about them between various entities.

Moreover, Article 35 provides another loophole that precludes notification "where laws or administrative regulations provide that secrecy shall be protected, or where notifications and obtaining consent will impede State organs' fulfillment of their statutory duties and responsibilities." The GDPR discusses secrecy in Article 90 but with an entirely different application.[222] In sum, the secrecy requirements of the final PIPL privilege state interests at the expense of individuals.

The PIPL's drifts toward favoring public and private institutions over the individual is consistent with expectations of an authoritarian regime. This is balanced by the right to redress in the courts (Article 50) that remains to be exhaustively tested.

[222] In the EU case, the secrecy clause allows member states to set out the powers of supervisory authorities who oversee data controllers or processors subject professional secrecy. The stated goal is to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules apply only to personal data which the controller or processor has received because of the obligation of secrecy.

The right to have one's data erased is an unresolved contradiction in the law. If the government insists that private sector firms surrender data to them, but individuals have already requested that the data be deleted, then it cannot be forwarded to the demanding authorities. It may be resolved through direct government data collection covering the same information set. For example, introducing a digital currency would allow government officials to access an individual's purchases, enabling them to access an individual's purchases and circumvent the financial service broker who facilitates the transaction.

4.8.4 Fragmented Authoritarianism

Finally, there is the policy implication of the PIPL for government entities. They are both an enforcement arm of the PIPL and a subject of the PIPL. The extent of law enforcement against government agencies remains to be seen. Like the threat of an anti-corruption campaign, the legal mechanism hangs over the heads of state officials like the sword of Damocles.

The fractured nature of China's autocratic rule is the subject of extensive academic literature that is too broad to review within this thesis's scope. Fragmented authoritarianism, a concept originally coined by Kenneth Lieberthal, refers to the idea that Chinese leaders do not behave in lockstep.[223] It is fragmented vertically, meaning that local or provincial officials do not often implement edicts from the central government. It is also fragmented horizontally, meaning that ministries and agencies have policy preferences at every level of the government.[224] Researchers often cite the example of environmental regulation as a node of fracture within

[223] Kenneth G. Lieberthal, ""Introduction: the 'fragmented authoritarianism' model and its limitations,"" in *Bureaucracy, Politics, and Decision-Making in Post-Mao China*, ed. Lieberthal and David M. Lampton (eds.) (Berkeley: University of California Press, 1992).
[224] Dickson, *The Party and the People: Chinese Politics in the 21st Century*.

the Chinese leadership. While one local agency will be incentivized to promote central government mandates because they represent a rural area with high agricultural output, another ministry will promote infrastructure projects that may occur at the expense of the environment and agriculture.

Fragmented authoritarianism 2.0, a term coined by Andrew Mertha, defines the Hu Jintao era. Under Hu, CCP authoritarianism allowed for input from civil society actors and NGOs, who brought new ideas of governance and could—to some degree—deliver government services. Another variant of this literature is "flexible repression," through which the party-state could allow for the mobilization of civil society without allowing the masses to emerge.[225] These models both allow for a degree of policy entrepreneurship. These features would be consistent with the NIA model described by Farrell and Newman. Consultative-style governance was significantly curtailed when Xi Jinping came to power. For example, Xi explicitly sought to stamp out any Western-influenced policy entrepreneurship from NGOs and other civil society actors when he introduced the NGO law in 2016. Foreign NGO operations, mostly staffed by local Chinese, were previously not well-regulated. While initially described as an attempt to survey and better control the "wild West" of foreign NGO work that had developed in the mainland over the decades since opening up, in reality, it has led to the departure of many foreign NGOs altogether.[226]

[225] Fu, *Mobilizing without the Masses: Control and Contention in China*. See also S. Heilmann and E. Perry, "Embracing Uncertainty: Guerilla Policy Style and Adaptive Governance in China," in *Mao's Invisible Hand: The Political Foundation of Adaptive Governance in China*, ed. S. Heilman and E. Perry (Cambridge, MA: Harvard University Press, 2011).

[226] "Fact Sheet on China's Foreign NGO Law," The China NGO Project, updated November 1, 2017, accessed March 10, 2022, https://www.chinafile.com/ngo/latest/fact-sheet-chinas-foreign-ngo-law.Statistics provided by the government yield an opaque picture, but the trend is clear. COVID is likely to have exacerbated the departures.

The PIPL creates an instrument to curtail the forces of fragmented authoritarianism. It holds local and provincial authorities accountable for the citizen data they store, a tool through which (however arbitrarily) the central government can justify punishing officials in ways that are palatable in the eyes of public opinion. Through this legal mechanism, the central government can purport to intervene on behalf of individual citizens whose local officials are either neglectful or incompetent or who are possibly abusing their power. One specific feature of the PIPL targeted at blunting power fragmentation is a key difference from the GDPR. Specifically, it holds *individuals* within the entity accountable and can fine them up to approximately $15,000 for any breach of the rules. There is no specification as to what constitutes a single instance of breach, meaning that the fines could quickly escalate. The GDPR, by contrast, allows for fines of a legal entity rather than an individual doing work in an official capacity. A further weapon against local officials is Article 69:

> "Where the right and interests of personal information are infringed upon due to personal information processing and cause damages, and the personal information processor *cannot prove that it is not at fault*, it shall bear the tort liability for damages.
>
> Liability for damages prescribed in the preceding paragraph shall be borne in light of the losses thus caused to the individuals concerned or the benefits thus obtained by the personal information processor; if the losses thus caused to the individuals concerned or the benefits thus obtained by the personal information processor are difficult to be determined, the *people's court shall determine the amount of compensation according to the actual circumstances*."[227] *(italics = author emphasis)*

[227] *China's Personal Information Protection Law: A Comparison of the First Draft, Second Draft, and the Final Document*.

With such a law in place, it is hard to imagine who would have the courage to sign up for the position of data protection officer in a government institution. The second provision allows for the People's Court, which is distinctly subordinated to the CCP, to determine compensation and rings especially ominous in the absence of ruling guidelines. Such guidelines will likely emerge in the coming years.

4.9 Conclusion: The Brussels Effect in China

The PIPL took effect in November 2021, so much about its implementation and enforcement remains nascent and unresolved. However, what does the China case show about the Brussels Effect? In its strictest sense, Europe's GDPR served as a legal template for China and, therefore can be counted as an example of the Brussels Effect. Yet, the outcomes intended by the GDPR, especially its focus on human rights, are clearly not reflected. Although China preserved much of the GDPR framework, it has unsurprisingly subordinated privacy as a human right to the rule of the Communist Party. China had traditionally understood privacy as a matter of protecting one's reputation. Yet, by using the Western human rights terminology and embracing data privacy regulations like the GDPR, China successfully coopts the language of liberal democracies and creates semantic confusion. China has frequently and sometimes inconsistently argued that the right to development dominates human rights at this stage of China's development. [228] In essence, signing on to Western-style privacy laws yet adapting them to suit Communist Party objectives is consistent with China's balance between participating meaningfully in the global system while seeking to rewrite its accepted norms simultaneously. By

[228] "Development as a human right : legal, political, and economic dimensions."

adopting GDPR-like privacy rules, China is following the same playbook as it has with the human rights narrative.

From the evidence presented here, China's manifestation of the Brussels Effect might also be understood as what Margaret Pearson referred to as "institutional isomorphism," i.e., the same institutional form adopted but with very different ancestries in each country and, ultimately, different outcomes.[229] In this sense, China's leaders have used the PIPL to bolster the legitimacy of the CCP. Not only does it form a part of a modern bureaucratic state, but it uses the law to encourage feedback to governing bodies that provide social services. In this way, China addresses the common problem of the dictator's dilemma, resulting in authoritarian governments failing to make sound policy choices owing to poor information flows. It also opens its legal system to Chinese citizens, giving them a venue to air grievances against the private sector. As with many policies China-related policies, it is an innovative approach to authoritarian rule and one that may prove successful.

[229] Margaret Pearson, "Variety Within and Without: The Political Economy of Chinese Regulation," in *Beyond the Middle Kingdom Comparative Perspectives on China's Capitalist Transformation*, ed. Scott Kennedy (Palo Alto: Stanford University Press, 2011). Pg. 28

5 Chapter V: United States & the NIA

From Concessionary Agreement to the Brussels Effect to Durable Arrangement?

5.1 Introduction

On March 30, 2022, Joe Biden and Ursula von der Leyen announced that the EU and the US had reached an updated version of the Privacy Shield agreement meant to settle the long-standing struggles between the two jurisdictions over cross-border data flows.[230] Its initial version is an agreement in which the United States has finally and meaningfully taken steps to reconcile differences in its legal system with the requirements of the EU privacy laws. This chapter tells how the GDPR specifically catalyzed the US adoption of European rules, thereby overturning decades-long resistance to a global convergence on more comprehensive and prescriptive data governance. It continues the transatlantic data flow narrative introduced by Farrell and Newman through their New Interdependence Approach (NIA). In their book *Of Privacy and Power*, the authors describe the earlier data transfer negotiations between the US and EU. They theorize how security actors across the two jurisdictions had access to power that allowed them to push through an agreement that did not comply with the EU *Charter of Fundamental Rights*. The March 2022 EU-US agreement is the culmination of many events and their interplay in the interim between the deals. The outcome of the new agreement, which some proponents have tongue-in-cheek dubbed "TADA" (the Transatlantic Data Agreement, though it has not officially been named yet), validates the NIA but with some twists along the way. The major twists

[230] "European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework," news release, March 25, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.

include, first, the reaction of corporations and the move by legislators to take on privacy legislation at the state level. The second twist was the unanticipated action by Congress in June 2022 to introduce the American Data Privacy and Protection Act (ADPPA). After many failed attempts, the ADPPA is the first bicameral and bipartisan proposal that comprehensively addresses major sticking points in the EU-US data transfer relationship. If passed, the law would bear many of the hallmark features of the GDPR. Taking into account these various strands of legislative effort, while the federal level developments validate the NIA, there are also elements of the Brussels Effect at work at the corporate and state level. Despite these monumental shifts, the ideational conception of data privacy as a human right *per se* has gained little currency in the U.S. Instead, data privacy has come to be articulated as a civil liberty.

5.2 Chapter Approach

This case study is different from the others because the next major development in the EU-US cross-border data transfer relationship remains unsettled. Emerging legislative developments in the United States are the empirical basis for testing the theoretical frameworks even as the story continues to unfurl. Hence, methodologically this chapter relies on primary documents, interviews, and news sources for information rather than on an exhaustive academic literature review. Beyond the theoretical differences, the China and Japan chapters focused largely on commercial data flows, whereas the US-EU story after the Snowden revelations centered on the linkage between commercial sector data and national security. This linkage became a key fulcrum of change in the Executive branch of the U.S. government. EU-US commercial data flows were well established through the Safe Harbor agreement struck in 2000 and continue to be so through the standard contractual clauses described in Appendix 3. Through

Safe Harbor, negotiators were able to segregate conceptually EU-U.S. data flows for national security and those for commerce, despite the passage of controversial legislation after 911 that allowed US national security officials to access private sector data.[231] Yet, as mentioned previously in Chapter II, Casper Bowden had frequently pointed out that the Safe Harbor agreement failed to acknowledge the link between commercial data collected by US firms on EU citizens that was subsequently shared with government officials. While in this chapter commercial data flows remain an important part of the story, the government access aspect played a catalytic role in forcing a shift in US resistance to European-style data privacy rules. Critical ideational shifts went along with the data governance regime emerging today.

Theoretically, this chapter incorporates the framework of both Farrell and Newman's New Interdependence Approach (2019) and the Brussels Effect outlined in Chapter II. It also references the work of Parsons and Matthijs (2021) for an ideational approach that is usefully applied to describe the differences between the EU and US conceptions of data privacy and protection and how these factors influence outcomes. These theoretical frameworks map onto an unfolding narrative that consists of three channels influencing the potential outcome of data regulation in the U.S. A visual diagram of these three channels is shown in Figure 2.

[231] Farrell and Newman, *Of Privacy and Power*. Pg. 136. An EU Commission study concluded that the US Patriot Act was "essentially irrelevant for [Safe Harbor] data flows."

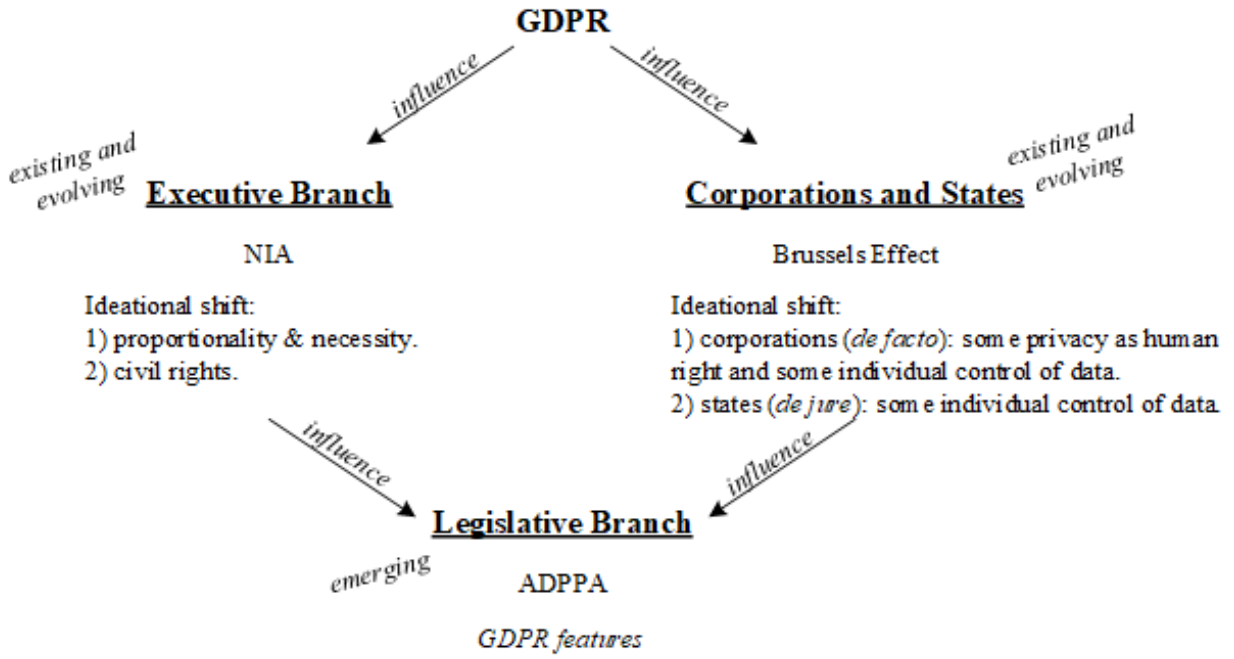

FIGURE 2: GDPR TRANSMISSION CHANNELS IN THE US

The first channel is the initiative of the Executive branch of government, whose Transatlantic Data Agreement with the EU will result in an EU adequacy finding if executed. The NIA explains the logic of the Safe Harbor agreement and the Privacy Shield and the Transatlantic Data Agreement. However, the new agreement would no longer be a *concessionary agreement*. Instead, it would fall into the category of a more *traditional adequacy* finding like that of Japan. This is because the US would have changed its law to accommodate the specific requirements of the European Union.

The second channel for regulatory change is that of state level data privacy legislation as well as the corporations that have adopted GDPR-like rules across their global platform. The state and corporate level channels are best explained by the Brussels Effect, in that firms and states adopted GDPR-like standards independent of their relationship with the EU. To be sure,

while the degree of the Brussels Effect can be disputed, there are several measures by which its explanatory power is evident.

The final channel is the ongoing effort at the Congressional level to pass federal data privacy legislation. It is also evidence of how cross-national layering generated legislative change, as predicted by the NIA. General transnational agreement on data privacy rules gradually rendered the US lack of action untenable for reasons linked to the European Court of Justice's ruling invalidating the Privacy Shield and voter concerns. If the proposed federal level legislation is passed with modifications acknowledging non-US citizens' rights, it is possible that the United States would achieve EU adequacy status without signing the Transatlantic Data Agreement. Collectively, these three conduits point in the direction of a U.S. data privacy and protection framework far more closely aligned with Europe than would have been possible under the U.S.'s previously more market-driven approach to data governance.

In each of the three channels, the United States shifted important views on data privacy and protection to enable change. At the Executive branch level, the government incorporated conceptions of proportionality and necessity not present in US legal parlance but very important to European jurisprudence. In addition, although it is not mentioned in the draft Transatlantic Data Agreement, the Biden administration has acknowledged the importance of linking privacy and human rights by spearheading the global *Declaration for the Future of the Internet* in 2022. While the administration stops short of declaring data privacy a right, as does the EU, it draws closer to this understanding in that declaration. At the corporate and state levels, greater individual control of data and how it is processed and stored by companies gains greater currency. Many multinational corporations openly adopt the language of data privacy as a human

right. Despite this adoption, most companies still dodge the human rights conceptualization. Finally, the federally-proposed ADPPA incorporates many GDPR concepts and features that would treat data privacy as a human right without using that language.

5.3 Broad Ideational Differences

What can explain the long-standing American resistance to the adoption of comprehensive data privacy rules such that it took enforcement from the European Court of Justice (ECJ) to cause the major shift? Exploring this question helps illuminate how the GDPR is changing the US approach to data governance. The origins of the difference were suggested in Chapter II and Chapter IV's China case study discussion of the Polanyian versus Hayekian approaches to political economy. When the internet emerged, the Clinton administration sought a light regulatory touch to allow the internet to flourish so that it could drive economic growth for decades to come, as pointed out by Farrell and Newman.[232] The Clinton administration's stance was not unique. It reflected systemic thinking woven across U.S. administrations regardless of their political affiliation. "The commitment to the relatively light regulation of digital firms and the Internet more broadly is akin to the constitutional hurdles to more government involvement in the domestic networks, but the limitation here is cultural or ideological, not legal,"[233] note cybersecurity experts Jack Goldsmith and Stuart Russell. Matthijs and Parsons' comparative framework thus provides a useful contextual explanation for the US's approach to data governance compared to Europe. In the authors' words:

[232] Farrell and Newman, *Of Privacy and Power*. Pg. 130.
[233] Jack Goldsmith and Stuart Russell, "Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations," *Aegis Series Paper No. 1806* (2018).

> *"Our account highlights contingent connections that political movements in each arena forged between ideas about markets and governance, creating distinct "varieties of neoliberalism" in the late 20th century. In continental Europe, neoliberalism found little initial purchase in national contexts but dovetailed with the mid-century project of European integration. Pro-market thinking came to be focused on strengthening central authority to eliminate interstate barriers. In America, neoliberals found common cause with social-conservative reactions to progressives' mid-century expansions of federal power. Pro-market thinking became a project to weaken central authority, promoting "states' rights" and downplaying or legitimating many of the same interstate barriers."*[234]

Both pro-market thinking and resistance to federal authority figure into US opposition to a federal data privacy law. The result is that "in practice, whenever sectoral legislation is not applicable, data privacy is mostly a matter of contracting between customers and businesses," as Jens Frankenreiter notes.[235] Matthijs and Parsons observe that the standard academic view of the EU as an "incomplete" market actually applies more to the U.S. than to the EU. The EU is more commercially integrated than the U.S. and, indeed, US state laws actively deter intrastate commercial flows. "Americans retain many costly interstate barriers that Europeans have either removed or reduced across their famous "four freedoms": the free movement of goods, services, capital, and people. Relatively greater cultural and institutional homogeneity and norms of mobility encourage Americans to trade and move across state lines despite such barriers, not because of their absence."[236]

Matthijs and Parsons' analysis of the U.S.'s internal market competition regulation can also be usefully applied to data privacy regulation dynamics. The fragmented nature of US interstate commerce is mirrored in data regulation. While the U.S. Congress has the legislative

[234] Matthias Matthijs and Craig Parsons, Why Did Europe's Single Market Surpass America's?, April 27, 2021.
[235] Frankenreiter, "The Missing 'California Effect' in Data Privacy Laws." Pp. 24.
[236] Matthias Matthijs and Craig Parsons, "Single-Market Power: How Europe Surpassed America in the Quest for Economic Integration," *Foreign Affairs* May/June 2022.

capacity and the Federal Trade Commission (FTC) has the deep administrative resources to facilitate harmonization and enforcement of data privacy rules, they have achieved comparatively little in their efforts to do so.[237] Some 17 consumer privacy bills have been proposed in the 2021-22 Congress alone.[238] These are supplemented by dozens of additional bills to address niche aspects of privacy and data protection at the sector level, including financial services, health, children's data, and government restrictions. None of these has risen to the level of a comprehensive law. And as with interstate commerce, Congress's lack of federal action has prompted states to take the lead in regulating data privacy.

So, on the one hand, we see U.S. states acting consistently with the old behavioral models that resist centralized regulation. On the other hand, we see the outside force of European regulatory preferences filling a conceptual framing gap at the state level where the U.S. Congress has failed to act. State legislation is where the NIA leaves off and the Brussels Effect takes on a stronger explanatory role. *Ironically, it is through the fragmented process that European data protection preferences gained currency and caused a general drift toward regulatory-driven data governance.* To be sure, there are still elements of the NIA at work in state legislatures, as EU officials have been in contact with state officials to influence outcomes in ways explained by the NIA. There has been close conversation between California officials and the European Commission.[239] A case-by-case study of the interaction between Brussels and state

[237] There are eight federal level privacy laws, all of which are sectoral rather than comprehensive: Children's Online Privacy Protection Act; Communications Act of 1934; Computer Fraud and Abuse Act; Consumer Financial Protection Act; Electronic Communications Privacy Act; Fair Credit Reporting Act; Federal Securities Laws; Federal Trade Commission (FTC) Act, which prohibits "unfair or deceptive acts or practices"; Gramm-Leach-Bliley Act; Health Insurance Portability and Accountability Act; Video Privacy Protection Act.
[238] https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/
[239] DeNardis and Murphree, interview.

legislators is beyond the scope of this thesis. What is noteworthy is the degree to which the NIA has forced ideational shifts compared to the Brussels Effect. Ideational questions are explored later in this chapter.

5.4 Concessionary Agreements

Weaving the idea from Chapter III of *concessionary agreements* into the narrative, this case study argues that both the Safe Harbor Agreement and the subsequent Privacy Shield signed in 2016 yielded pseudo-adequacy arrangements insufficient to the European data privacy directive requirements in force at the time. The agreements both represented profound concessions on the part of the EU that primarily reflected the preferences of security advocates within the EU who sought to circumvent their internal privacy constraints, as shown by Farrell and Newman in their analysis of Wikileaks documents and other sources. The agreements did not incorporate the protection mechanisms required to ensure the EU's dignitary approach to privacy as would be necessary for a traditional adequacy finding like the Japan case study. In addition, the United States did not make changes to its legal system to secure adequacy status from the EU. By this definition, both the Safe Harbor and Privacy Shield agreements were concessionary in nature. Officially, the United States was granted an adequacy decision. Nevertheless, it was clear from the beginning that the data privacy safeguards put in place by the agreements were far from living up to the European *Fundamental Charter of Rights*. Were the Transatlantic Data Agreement to pass, it would follow a model more closely aligned with a traditional adequacy finding, although it would still be theoretically explained by the NIA. The TADA would not constitute a concessionary agreement.

The passage of the GDPR in 2016 narrowed, if not eliminated, the capacity of the European Commission to strike concessionary agreements. It opened a two-pronged attack on the US privacy framework. First, the GDPR strengthened the position of privacy activists in Europe to exercise veto power over EU-US data privacy negotiations. When the GDPR took effect in 2018, Max Schrems and his organization, *nyob* (none of your business), challenged the EU-US agreement in the ECJ. Through the ECJ, Schrems was able to *defend* European regulatory preferences and indeed, *extend* them to the United States, as is featured in the NIA. When the ECJ ruled in favor of the Schrems, this created a moment in which the Brussels Effect could dominate—firms and US states voluntarily rolled out higher data protection standards, even as actors elsewhere at the federal level continued to function in ways consistent with the NIA. With the demise of the Privacy Shield, the ECJ and those who accessed it to defend European privacy laws became the political actors who assumed influence at the expense of European and US security advocates. Negotiators from the European Commission and the U.S. Department of Commerce responded to this new set of actors as they sought to find a new solution to cross-border data flows. By accessing the courts to enforce the *Charter of Fundamental Rights*, privacy groups not only shifted the attitude of major US tech firms toward accepting the dignitary conception of data protection, but ultimately required that the US make concessions despite the market dominance of US technology and social media in Europe.

Second, the broadening of the extraterritorial reach of the GDPR affected a wider group of US companies than the 1995 Data Privacy Directive had previously impacted. The expansion of the territorial span was discussed in Chapter II. Compliance with the GDPR forced corporations to consider the implications of a human rights approach to data privacy at the operational

level. Large multinational companies, in part responding to the nullification of the Privacy Shield, started to adopt the standards across their global platforms. This happened in varying degrees as will be discussed. It also increased the number of US companies incentivized to advocate for stronger national-level data privacy protections within the US for the purposes of global harmonization. Recalling Chapter III, the desire for harmonization creates the conditions for the Brussels Effect to occur. MNCs started to lobby federal legislators to adopt more robust data regulation, arguing that it served the interest of business efficiency.[240] Thus, while firms responded to the ECJ ruling in ways predicted by the NIA, their response also bears the hallmarks of the Brussels Effect. That is, some firms voluntarily rolled out higher data protection standards across their global platforms rather than simply complying with EU rules in the specifically affected business units. Thus, the US case bears out the uni-directional nature of the Brussels Effect in accounting for the GDPR's diffusion at the corporate level in the United States. That is, while EU standards were adopted in US jurisdictions, it was not the case that the EU softened its domestic data privacy rules, as might be predicted by the NIA.

The research now turns to the specific instances of GDPR-like regulation adoption through the three channels outlined in the introduction.

5.5 NIA: Safe Harbor & the Privacy Shield

The Safe Harbor shows how both the US and the EU sought to defend and extend their data protection preferences in their negotiations with one another. The final agreement began as an exchange of letters that resulted formally in an adequacy finding by the European Union.

[240] Alfred Ng, "Tech giants ask Congress for a data privacy bill to bypass state laws," *CNET* (September 10, 2019).

The letters included a set of Safe Harbor Principles that were based on the 1995 Data Privacy Directive. Firms would be required to sign up to those principles and submit to enforcement by either self-regulatory bodies or the FTC in cases of disputes. The FTC would adjudicate disputes between European citizens and firms that had signed up to the Safe Harbor. The Europeans had the right to block flows to corporations that were in breach of the Safe Harbor principles.[241] These were the three basic features of the agreement. They papered over many key areas of concern to privacy actors. For example, the United States did not institute an independent data protection body, nor did EU citizens gain the individual right to redress. As Farrell and Newman note, "from the perspective of the actual negotiators, Safe Harbor was a success, protecting the existing institutional arrangements of each of the negotiating parties while avoiding a potentially serious dispute between them... While the United States could continue to claim publicly that its basic policy stance of protecting privacy through self-regulation was unchanged, the European Union could say that it had succeeded in dictating the terms of self-regulation." In the NIA framework, both parties could defend their existing domestic institutions. At the same time, both parties hoped they had planted a Trojan Horse in the other party's system. For the most part, the United States had successfully promoted its approach to financial markets in Europe, so the Americans had a precedent that suggested they could replicate their pro-market approach to data protection. From the perspective of the concessionary agreement model, the details of the Safe Harbor agreement showed how the EU gave the predominance of ground in negotiations.

[241] Farrell and Newman, *Of Privacy and Power*. Pg. 132.

It took the Snowden disclosures in 2013 to unmask just how much ground the Europeans had given. The revelations substantiated broad concerns within the EU about the scope and reach of U.S. surveillance activities, as discussed in Chapter II. It also opened the door for Maximilian Schrems to file a complaint with the Irish Data Protection Commissioner (DPC), which he did in June 2013. In this complaint, Mr. Schrems challenged the validity of the Safe Harbor agreement as applied by Facebook in a case colloquially referred to as *Schrems I*. He noted that under US law, his personal data could be transferred from Facebook Ireland Ltd. to its US parent company and then later be accessed by US security agencies, especially the US National Security Agency (NSA), which operated a surveillance program called "PRISM."[242] The DPC declined to investigate the complaint. Schrems appealed this decision before the Irish High Court, which in turn referred the following questions to the European Court of Justice for a preliminary ruling. The DPC asked the ECJ to rule on: (1) Whether a data protection authority, in the course of investigating an individual's complaint that personal data is being transferred to another country where laws and practices do not provide adequate protections for the individual, is absolutely bound by the Safe Harbor Decision of the European Commission, or;[243] (2) whether the data protection authority is required to conduct its own investigations taking into account factual developments, or whether this authority lies elsewhere. In October 2015, the ECJ ruled that national authorities have the right to investigate individual complaints related to Commission decisions and legal instruments.[244] It also declared that *only* the ECJ is authorized to

[242] "NSA Prism program taps in to user data of Apple, Google and others," (2013). https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
[243] The court referred specifically to the provisions of Article 25(6) of Directive 95/46 and Articles 7, 8 and 47 of the European Charter of Fundamental Rights (ECFR).
[244] "Judgement of the Court," ed. Court of Justice of the European Union (2015). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362.

declare an agreement such as the Safe Harbor invalid. Finally, the ECJ declared the Safe Harbor agreement invalid on the grounds that the European Commission exceeded its powers by making a shortcut on the adequacy procedure. In other words, the court agreed that the Safe Harbor was a *concessionary agreement* that was grossly inadequate to protect EU citizen data.

The court's findings were a complete game-changer for privacy advocates on several fronts. First, it tightened the meaning of "essentially equivalent" domestic laws by virtue of which third countries could attain adequacy status. This partly meant that exemptions for national security must comply with the European legal principle of proportionality and allow EU citizens to seek relief in the courts for abuses. The court's ruling thus narrowed the scope of allowable exemptions for national security purposes. Second, the ruling made the ECJ the ultimate arbiter of future adequacy arrangements negotiated by the Commission. Individuals, such as privacy advocates, gained the power to challenge Commission adequacy determinations through the courts.

Ironically, the concerns raised by privacy advocates after Snowden had resulted in important changes to the U.S. legal framework for surveillance prior to the ECJ's 2015 ruling, but ultimately not in ways that would satisfy the European Parliament or the ECJ. For example, in 2014 US President Obama issued the *Presidential Policy Directive 28*, which applied to U.S. signals intelligence activities and extended certain privacy protections to all people, regardless of location or nationality.[245] In 2015 Congress also enacted the *USA Freedom Act*, which among other things, prohibited the use of key national security authorities to conduct bulk

[245] Presidential Policy Directive -- Signals Intelligence Activities, (The White House, 2014).

collection.[246] In addition, the U.S. intelligence community launched a strategic effort to provide an unprecedented degree of transparency.[247] As Farrell and Newman note, "US officials believed that the European Court of Justice has gotten the facts wrong, and was basing its rule on an understanding of privacy law and practice that was both incorrect and badly out of date, given post-Snowden reforms."[248]

In light of *Schrems I*, negotiators returned to the drawing board for an agreement to replace Safe Harbor. For EU representatives, the ECJ ruling gave them the cover they needed to take a harder line with US negotiators, and they did so. To counteract this harder stance, the US negotiating team included not only staff from the U.S. Department of Commerce, but more importantly included the direct involvement of Robert Litt, the US's general counsel for the Director of Intelligence. He had the expertise to address the US's legal guardrails around data sharing for national security purposes. Those negotiations resulted in the Privacy Shield, signed in July 2016. The new agreement involved more robust and transparent monitoring and enforcement of cross-border data transfers, gave European officials more authority to press unresolved violations, and also established better dispute resolution mechanisms.[249] Of these concessions, perhaps the most important one was the creation of an ombudsman position, which would receive complaints from EU citizens who felt their privacy has been violated. However, the concession lacked substance. EU officials were deeply dissatisfied with the arrangement, and most agreed that it would not stand up to review by the ECJ. As many observers point out, the

[246] USA Freedom Act, (2015).
[247] https://www.prismrisk.gov/about-prism/prism-transparency/
[248] Farrell and Newman, *Of Privacy and Power*., pg. 151.
[249] Farrell and Newman, *Of Privacy and Power*. Pg. 153-54.

Privacy Shield still represented a watered-down version of the EU's extant privacy laws. One observer noted, "This new Privacy Shield is not going to stand up in court…. It's political fiction."[250] Thus, as soon as the GDPR took effect in 2018, Max Schrems returned to court with a new legal challenge, colloquially referred to as *Schrems II*. In June 2020, the ECJ found the Privacy Shield invalid. The next section discusses the specifics of the ECJ's findings in *Schrems II*.

5.5.1 Legal and Ideational Differences

Why did the U.S.'s legislative and enforcement changes not rise to ECJ's interpretation of the EU *Charter on Fundamental Rights*? The similarity between the US and EU democratic political systems masks profound philosophical differences in their approach to legal dispute resolution writ large. The first and second Schrems cases brought these differences into dramatic relief. The EU's regulatory system is based on the precautionary principle, which puts rules in place to anticipate and preempt harm.[251] By contrast, the US's system seeks to address harm after the fact through tort law. Thus, US commercial law allows businesses *by defaul*t to gather, process, and share information that they obtain from their customers. Chapter II discussed the sectoral regulation of industries in the United States. Beyond sectoral regulation, the Federal Trade Commission (FTC) has the authority to clamp down on bad actors who engage in deceptive or unfair practices. However, the FTC can only act once it has enough evidence to show that actual harm has been done. For individuals, the U.S. legal system is based on the principle of rectifying or redressing harm after the fact as well, but individuals must

[250] Wayne Rash, "EU, U.S. Privacy Shield Deal Greeted With Claims It's Meaningless," Article, *eWeek* (2016).
[251] "The Precautionary Principle," in *European Encyclopedia of Law: European Union Regulations*. https://europeanlaw.lawlegal.eu/the-precautionary-principle/.

demonstrate that they have been personally and *directly* injured by data collection.[252] This is a legal hurdle that is very hard to clear in privacy cases involving massive data collection for consumer market insight or preferential pricing. The individual would have to prove that personal data collected about him or her directly led to price discrimination against them individually. It is a subject of academic debate as to whether the EU is in fact more likely to apply the precautionary principle than the U.S.[253] However, in the case of privacy, the EU adopts the more conservative precautionary approach. In the eyes of the EU, the U.S.'s legal precedents around data privacy, which historically require individuals to prove personal injury caused by privacy violations, are not adequate to reflect the nature and potential damage of online data gathering. The philosophical difference between the two legal systems thus explains why the Brussels Effect alone could not be the mechanism through which European data protection standards would spread to the United States. Some external coercion from the EU was required.

After the *Schrems II* ruling, many US legal scholars adamantly defended US protections, arguing that guardrails on US government surveillance were more robust than that of many European nations.[254] The European Court of Justice's findings reflected that even though the United States had made important changes to its domestic legislation vis-à-vis government surveillance, several key aspects remained unfulfilled. The court found that "limitations on the

[252] *U.S. Private-Sector Privacy (Participant Guide)*, (Portsmouth, NH: International Association of Privacy Professionals, 2021).
[253] For discussion of this topic, cf. Marco Bocchi, "Is the EU really more precautionary than the US? Some thoughts in relation to TTIP negotiations," *Blog of the European Journal of International Law*, August 9, 2016, https://www.ejiltalk.org/is-the-eu-really-more-precautionary-than-the-us-some-thoughts-in-relation-to-ttip-negotiations/.
[254] See, for example, Christopher Wolf, " Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers," *Washington University Journal of Law and Policy* 43, no. 1 (2014), https://openscholarship.wustl.edu/law_journal_law_policy/vol43/iss1/13. See also, Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms since 2013."*, Future of Privacy Forum (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709619.

protection of personal data arising from the domestic law of the United States on the access and use by US public authorities….are not circumscribed in a way that satisfies requirements that are *essentially equivalent* to those required under EU law, by the *principle of proportionality* in so far as the surveillance programmes [*sic*] on those provisions are not limited to what is *strictly necessary (italics = author emphasis)*."[255] The three key terms here *are essential equivalence, the principle of proportionality, and strictly necessary*. As Chapter III pointed out, the GDPR introduced the condition of essential equivalence. It requires that even though countries are not required to have exactly the same laws governing privacy as the EU does, they are required to achieve similar privacy and dignitary outcomes.

The principle of proportionality is one of the key analytical frameworks through which the ECJ evaluates essential equivalence. The principle of proportionality (and its associated requirement for strict necessity) is recognized in many other international legal systems, including Canada and the UK, but it has not traditionally been recognized in the US justice system. Under proportionality, the weight of analysis is less on whether a right has been identified—the US approach—and more on the government's justification for burdening the right. Proportionality enables courts to reconcile conflicting rights and norms by balancing their relative value. It requires that a government policy is genuinely targeted at a legitimate policy objective. It further requires that the government consider whether it could achieve the same policy objective in

[255] "The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield," news release, 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

ways that impose less of a burden on the individual right. Finally, the government must show that its policy does not disproportionately burden a given right relative to the objective.[256]

Since the 1960s civil rights movement, the United States Supreme Court has *de facto* eschewed the principle of proportionality. It has instead weighed the value of one right against the other and has issued verdicts that ultimately result in the nullification of one right over another.[257] In the controversial decision in Roe v. Wade in the 1970s, for example, the court ruled that fetuses do not have constitutional rights. Justice Harry Blackmun, Roe's author, "thought denying fetal rights was the price of saying women had the right to control their bodies. Either women had constitutional rights or fetuses did. There was no middle ground, no room for compromise," notes Columbia law professor Jamal Greene.[258] In Greene's book, *How Rights Went Wrong*, the author outlines a series of Supreme Court cases that show a historical trend toward adjudicating between two rights by eviscerating one of the two, with the result that the courts can often "sever rights from justice."[259]

The importance of this US tradition has been an operational feature of the collision course between the US and the EU over data privacy and protection. In overturning *Roe v. Wade* in June 2022, the Supreme Court's ruling opinion pointed out that the U.S. Constitution does not specifically guarantee a right to privacy, thereby negating that right in the context of abortion. On those grounds, the Court returned the abortion question to the states. Returning the decision to the states encourages the fragmentation seen in data privacy regulation today.

---

[256] Wolf Sauter, "Proportionality in EU Law: A Balancing Act?," *Cambridge Yearbook of European Legal Studies* 15 (2013), https://doi.org/10.5235/152888713809813611.
[257] Jamal Greene, *How Rights Went Wrong* (New York: Houghton Mifflin, 2021). Pg. xv.
[258] Ibid, pg. xv.
[259] Ibid, pg. 111. For a detailed discussion of how Germany navigated the competing right of a woman to choose versus the right of the fetus, see Chapter 5, "When Rights Collide."

Without ideological access to the principle of proportionality, many states have since adopted highly restrictive abortion laws that swing the pendulum in the direction of eviscerating the woman's right to make a (private) choice in favor of rights inferred to a fetus. That is, the either/or tendency of the Supreme Court is being replicated across the states. Privacy issues have historically defied either/or logic. Thus, there will undoubtedly be a Supreme Court case within the next decade that will evaluate privacy issues in the context of the right of states to access software applications that could prove a woman had sought an abortion when she is a resident of a state where such a procedure is either highly proscribed or totally illegal.[260] Such a practice directly conflicts with the Supreme Court's long-standing tradition of imposing guardrails around government or public access to private information.[261] Access to the proportionality principle is thus an important tool missing from the US tool box for protecting privacy as a human right.

Besides the ECJ's ruling on the major legal/conceptual differences that nullified the Privacy Shield, the court also ruled that: 1) the agreement did not include *effective* mechanisms for the enforcement of data transfers, and; 2) individuals did not have a *de facto* ability to seek individual redress in US courts through the ombudsman feature. In short, the ECJ rejected virtually all the putative concessions made by U.S. officials in the replacement to the Safe Harbor agreement. The March 2022 Transatlantic Data Agreement marked a major change in the US position, as the next section shows.

---

[260] Taylor Hatmaker, "Congress probes period tracking apps and data brokers over abortion privacy concerns," (TechCrunch, July 8, 2022). https://techcrunch.com/2022/07/08/house-oversight-letter-abortion-period-apps-data-brokers/.

[261] This tradition was sparked with what has been referred to as the most influential legal article ever written: S.D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* IV (December 15, 1890), https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

5.6 NIA Redux: Transatlantic Data Agreement of 2022

The Transatlantic Data Agreement (TADA) *in principle* of 2022 represents a change in which the United States finally conceded to key objections of privacy activists in the EU after decades of resistance. The announcement by Joe Biden and Ursula van der Leyen showed how significant the topic of data transfers had become within Transatlantic affairs compared to the Privacy Shield announcement. When the Privacy Shield was struck, the deal was announced by the Commission Vice-President Andrus Ansip and Commissioner Vera Jourova announced in February 2016 rather than by the US president and the Commission president.[262] Moreover, while the Privacy Shield took six months to negotiate, TADA took two years, signaling that both sides were looking for a deal that would withstand challenge at the ECJ. When chief negotiators Bruno Gencarelli of the EU and Chris Hoff of the US Department of Commerce presented at the IAPP Global Privacy Summit in April 2022, they commented on how they had analyzed the Schrems II ruling line-by-line to address each point as they crafted the new agreement.[263] Key features of the agreement show how much the United States has moved toward the EU data governance model and is therefore consistent with outcomes the NIA would predict:[264]

[262] Catherine Stupp, "Commission replaces Safe Harbour with rebranded 'privacy shield'," *Euractiv*, February 3, 2016, https://www.euractiv.com/section/digital/news/commission-replaces-safe-harbour-with-rebranded-privacy-shield/.
[263] Bruno Gencarelli and Christopher Hoff, "EU-U.S. Privacy Shield and teh Future of Trans-Atlantic Data Flows," interview by Brian Scarpelli, *IAPP Global Privacy Summit 2022*, https://iapp.org/conference/past-conferences/GPS22/.
[264] "United States and European Commission Announce Trans-Atlantic Data Privacy Framework," news release, March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/. See also "European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework."

- The United States agreed to "implement new safeguards" to ensure that signals intelligence activities are "necessary and proportionate" (an EU legal measure under Article 52 of the EU Charter) to achieve national security objectives.

- The United States will also create a "new mechanism for the EU individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities." Redress would be affected through an independent Data Protection Review Court consisting of "individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed." This new mechanism addresses the EU's requirement for an independent and binding authority that had been absent in the Privacy Shield.

- Oversight of intelligence activities will be heightened, i.e., "intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards." Oversight and redress are different issues, but have historically have been described as being one and the same. Being addressed separately in the White House's announcement shows the degree to which negotiators sought to satisfy the ECJ.[265]

- The White House announcement includes several specifically EU legal concepts, besides necessity and proportionality, including privacy and data protection conceptually separated, and a legal basis for data flows. Legal bases are a core part of the GDPR but have not been recognized by the US until the TADA.

- The agreement frames safeguards for data flows as more than a trade or commerce issue, acknowledging the European approach to data protection. [266] It includes a "shared commitment to privacy, data protection, the rule of law, and our collective security as well as our mutual recognition of the importance of trans-Atlantic data flows to our respective citizens, economies, and societies."

- Addressing the EU *Charter's* assertion that surveillance and data protection are a fundamental rights, the proposed agreement will strengthen safeguards to protect "privacy and civil liberties." Civil liberties was a term not present in previous agreements. Civil liberties can be seen as a close cousin of human rights.

- The new framework will continue to be a self-certification scheme managed by the US Department of Commerce. Self-certification allows the United States to defend some of its existing institutions.

[265] For details on redress versus oversight, see Christopher Docksey, "Schrems II and Individual Redress—Where There's a Will, There's a Way," *Lawfare*, October 12, 2020, https://www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way.

[266] Compare the new agreement to the following statement by U.S. Department of Commerce, "Statement From U.S. Secretary of Commerce Penny Pritzker on EU-U.S. Privacy Shield," (Youtube: February 2, 2016).

The deal would require the Biden Administration to adopt an Executive Order that includes all these commitments and would form the basis on which the European Commission will draft an adequacy decision, as detailed in the White House press release. An Executive Order has the status of law in the United States, and in this sense the new TADA would fit conceptually more closely with a traditional adequacy finding rather than a *concessionary agreement*. An Executive Order does not require congressional action to assume legal force, nor can Congress overturn such an order. It is, however, a weaker form of legislative change, as an Executive Order can be overturned by a new president through a simple signature.[267] Because it is a weaker form of law, there is an argument to be made that the TADA is still a concessionary agreement. Either way, the evolution of EU-US data transfer agreements supports the NIA as a theoretical framework and shows how far the United States has moved in the direction of European data governance preferences. If the US Congress finally passes the proposed ADPPA with modifications to ensure protections for non-US citizens, the TADA would likely be unnecessary, and the question of concessionary agreements would be moot. The United States could instead secure an adequacy finding that would stand up to the ECJ scrutiny through the ADPPA.[268]

In sum, the Transatlantic Data Agreement shows a strong shift in the US executive branch approach to data privacy that was influenced by private actors outside of the United States. While at the federal level, the United States never embraced the language of human rights, many features of the new agreement reflect features and principles through which the

[267] Executive orders have the force of law, much like regulations issued by federal agencies, so they are codified under Title 3 of the Code of Federal Regulations, which is the formal collection of all of the rules and regulations issued by the executive branch and other federal agencies. https://www.americanbar.org/groups/public_education/publications/teaching-legal-docs/what-is-an-executive-order-/

[268] Some parties have questioned whether ADPPA protections would apply to EU citizens in its current wording. Presumably this would become a point of negotiation between the US and the EU.

European Union achieves its dignitary outcomes. Between the concessionary agreement and the long distance that the executive branch traveled to today, large US corporations started to voluntarily adopt aspects of the GDPR. The next section unfolds the details of this movement.

5.7 Brussels Effect and *de facto* GDPR adoption: Corporations

> *"The de facto Brussels Effect is particularly strong in the domain of data privacy…Various examples suggest that, for today's global digital companies, maintaining different data practices across global markets is often both difficult (due to technical non-divisibility) and costly (due to economic non-divisibility)."*
> *–Anu Bradford*[269]

The passage of the GDPR coupled with the successful challenge to the Privacy Shield resulted in a US business scramble to understand how data flows would proceed between the EU and US from that point on. During the period in which negotiators discussed replacing the Privacy Shield, the Brussels Effect took over as a mechanism for diffusing privacy regulation.[270] Many firms started to align themselves more closely with the GDPR in their US-based operations. The corporate context brings a different aspect of the Brussels Effect into relief than the legal prototype model described in the China chapter. In companies, the Brussels Effect describes the *de facto* adoption of European regulatory standards based on motivations related to cost efficiencies or consumer demand for higher data privacy standards. Another potential factor is the desire of large corporations to reduce the probability of regulatory scrutiny by adopting higher standards. Regardless of the motivation, adopting GPDR standards by corporates,

[269] Bradford, *The Brussels Effect*. Pgs. 142-43.
[270] Until a new arrangement is reached, U.S. companies will transfer data through the standard contractual clauses (SCCs) discussed in Appendix 3. In theory, SCCs uphold the GDPR standards, but they increase the costs of compliance, especially for small and medium-sized companies who do not have large legal compliance capacity. As a result of the Privacy Shield finding, the European Commission raised the compliance standards of SCCs to ensure that they too would not be subject to legal challenge.

especially the global social media and e-commerce platforms, is often cited as evidence of the Brussels Effect.

Amazon, Apple, Facebook, Google, and Microsoft all rolled the GDPR out on their global platforms to varying degrees.[271] These rollouts were conducted with great public fanfare. In 2018, Microsoft was the first firm to rollout a policy that adopted data privacy as a human right.[272] It was soon followed by Apple, whose privacy portals directly states, "Privacy is a fundamental human right."[273] Apple has implemented the most robust individual privacy policies, according to researchers Gunst and De Ville (2021). This is not surprising given that Apple does not rely on advertising for the bulk of its revenue stream. Apple's post-GDPR privacy features include settings that allow users to see and block advertisers from tracking their movement to different websites and location tracking that is erased quickly and does not associate a person's location with their Apple ID. Thus, to a significant extent, the corporate policies of both Microsoft and Apple reflect the spirit and features of the GDPR.

Other firms have also rolled out greater privacy options on their websites though they do not embrace data privacy as a human right per se. Anu Bradford has argued that technology companies would be required to raise their standards across the board because they would have difficulty segregating audiences or consumers in different jurisdictions—the principle of "non-divisibility" in her book.[274] While it is true that many companies raised their standards,

[271] Simon Gunst and Ferdi De Ville, "The Brussels Effect: How the GDPR Conquered Silicon Valley," *European Foreign Affairs Review* 26, No. 3 (2021).
[272] Julie Brill, "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data," *Microsoft on the Issues*, May 21, 2018, https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.
[273] "Apple Privacy Policy," accessed June 4, 2022, https://www.apple.com/privacy/.
[274] Bradford, *The Brussels Effect*. Pg. 142-43.

they did not do so because of non-divisibility. Facebook and Amazon, for example, have proven this is not the case. Before the GDPR, all of Facebook's users were legally part of Facebook's Irish subsidiary.[275] After the GDPR took effect, these users were moved to Facebook's California headquarters to circumvent the higher compliance standards of the GDPR. Facebook's non-EU version of its terms of service explicitly seeks to limit its liability by stating that its products are provided "as-is" with "no guarantees that they always will be safe, secure, or error-free."[276] Such a statement would not be allowable under Article 82 of the GDPR.[277] Both Facebook and Amazon.com have segregated their privacy policies by geography since the GDPR took effect. Amazon's post-GDPR privacy policy in the EU suggests that the company stopped using email tracking and location-based services. The US policy did not reflect the same changes.[278] In short, while all major e-commerce and social media platforms have raised their privacy standards, some companies have navigated the regulatory environment in ways that undermine the theoretical application of the Brussels Effect to some degree.

Quantitative research by Jens Frankenreiter questions how extensive the Brussels Effect has been in driving the adoption of European standards in the United States. While the evidence shows that the largest MNCs have taken on these standards and advocated for their adoption globally, smaller and mid-sized companies have not necessarily done the same. Frankenreiter's study of 695 non-EU websites concludes that the GDPR's influence on business

[275] Alex Hern, "Facebook moves 1.5bn users out of reach of new European privacy law," *The Guardian* (April 19, 2018). https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law.
[276] Gunst and De Ville, pg. 445.
[277] Art. 82 GDPR - Right to compensation and liability - GDPR.eu
[278] Frankenreiter, "The Missing 'California Effect' in Data Privacy Laws." Pg. 34. The author created a longitudinal data set of privacy policies before and after the GDPR took effect. He uses machine learning to analyze the semantic content of these policies to determine changes in privacy policy, if any.

operations outside the EU is "limited at best."[279] The author challenges the logic of the California Effect—the original theoretical framework that is the inspiration for the Brussels Effect. Specifically, he considers the cost-efficiency motivation for firms to adopt GDPR-like rules and shows that only a few firms adopted fully GDPR-compliant practices globally. From a group of 68 US privacy policies and their EU counterparts, Frankenreiter finds systemic differences in how US businesses with operations in Europe adjusted the privacy policies of US websites in reaction to the GDPR's entry into force. His findings further show that in one subset of firms, 44 out of 150 US-based company websites increased the level of protection to US consumers while 58 out of 150 websites extended preferential treatment to EU-based customers.[280] Thus, despite the considerable evolution of US thinking on data privacy and protection, a minority of U.S. companies fully implement the GDPR, much less embrace data privacy as a human right.

However, from the perspective of market capitalization, the number of customers, and overall global reach, Apple, Google, and Microsoft play an outsized role in influencing attitudes toward data privacy policy. Collectively, the three companies have a stock market capitalization of US$5.4 trillion, or 23% of US annual GDP. Active Apple smartphone units total 1.8 billion, or roughly 22% of the world's population.[281] Forty-five percent of Apple's revenues derive from the Americas, which suggests that a very large consumer base that is not directly governed by GDPR standards still enjoys the privacy benefits of the GDPR by virtue of Apple's global policy. Similarly, Microsoft has 1.2 billion active users of Microsoft Office as of 2020 in addition to 120

[279] Ibid, pg. 56.
[280] Ibid, pg. 50.
[281] Milica Arsenovic, "26+ Incredible Apple Statistics Showing Off Its Uniqueness " (April 7, 2022). https://capitalcounselor.com/apple-statistics/.

million business users.[282] Finally, while Google has not publicly embraced data privacy as a human right, the company offers privacy settings that extend considerable control to data subjects inspired by European preferences. For example, Google allows users to turn off personalized ads and location tracking. In addition, when they solicit consumer consent for data gathering, they limit the use of the gathering to the specified purpose rather than using that data for other "legitimate interests," a term directly from the GDPR lexicon.[283] US law does not currently require these controls and therefore represent a voluntary corporate policy. There is more that Google could do to fall in line with the spirit of the GDPR. The point is that these firms' massive scale can generate changes in market behavior. Customers of these extremely dominant companies may develop a strong preference for better privacy controls over time. They may even demonstrate a willingness to pay more for products with more comprehensive privacy features. Alternatively, horizontal transmission of GDPR standards can occur when dominant firms require key suppliers to comply with GDPR, as indicated in Chapter II. In this sense, the raw numbers of US firms adopting or failing to adopt GDPR standards may not be the most relevant measure of the Brussels Effect. By contrast, Facebook, through its relatively weak data governance practices, has further and repeatedly raised the salience of greater privacy protections.[284] While most Americans in a survey say they value privacy, comparatively little has been achieved

[282] "Microsoft by the Numbers," accessed August 25, 2022, https://news.microsoft.com/bythenumbers/en/homepage.
[283] "Google Privacy Policy US," accessed September 24, 2022, https://policies.google.com/privacy?hl=en-US#infochoices.
[284] Jeff Horwitz, "The Facebook Files," *Wall Street Journal* (New York), October 1, 2021, https://www.wsj.com/articles/the-facebook-files-11631713039.

to protect citizens' interests from the prying eyes of corporations in the digital universe prior to the GDPR.[285]

In sum, privacy policies among key economic actors across the globe increasingly expose consumers to more control over their data. While many businesses, especially US businesses, continue to argue for less consumer control, the general trend is moving in favor of consumers. For some businesses, like Apple, stronger privacy settings have become a competitive advantage. If other firms seek to leverage privacy settings as a competitive tool, we may see a tipping point reached whereby higher standards will become the norm rather than the exception.

More recently, technology and financial firms, among others, collectively began to push Congress for national level legislation. For example, in 2019, the Business Roundtable issued a public letter to Congress signed by more than 50 Business Roundtable CEOs across industries urging policymakers to pass a comprehensive national data privacy law.[286] The corporate call for a national data privacy law was partly driven by the trend in states to legislate privacy locally. State initiatives are the topic of the next section.

5.8 Brussels Effect: States

Since the 2016 passage of the GDPR, and especially since the nullification of the Privacy Shield by the ECJ in 2020, states have recognized the urgency of passing privacy laws. Today,

[285] Lee Rainie and et al, *Americans and Privacy: Confused, Concerned, and Feeling Lack of Control over Their Personal Information* (2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. This is in part because in the US privacy has in the past largely been articulated in terms of government rather than private sector prying into individual lives, as the Safe Harbor and Privacy Shield agreements show. For a deep review of this topic, cf. Sarah Igo, *The Known Citizen* (Boston: Harvard University Press, 2018).

[286] "CEOS to Congress: pass comprehensive nationwide consumer data privacy law ", (Business Roundtable, September 10, 2019). https://s3.amazonaws.com/brt.org/BRT-CEOLetteronPrivacy-Finalv2.pdf.

California, Colorado, Connecticut, Virginia, and Utah, have passed comprehensive data privacy laws that incorporate many European data privacy preferences. (See Table 3.) These collectively take effect in 2023. Moreover, in 2021, 38 states proposed roughly 160 consumer data privacy bills, according to a National Conference of State Legislatures report.[287]

California was the first state to pass such legislation in 2018. The California Consumer Privacy Act (CCPA) actively modeled its laws on the GDPR in consultation with European regulators.[288] The first version of the law reflected accommodations achieved through powerful Silicon Valley lobbying. For example, California conceded that firms could continue automated decision-making and could limit the individual's ability to seek redress in state courts. It also denied individuals the right to rectify incorrect information based on the argument that inaccurate information could be remedied by exercising the right to deletion already present in the law.[289] The updated version of the CCPA, the California Privacy Rights Act (CPRA) passed in 2020. This revised version encompasses all the rights and business obligations of the GDPR and overturns the previous concessions, save for automated data processing.[290] It adds the right to

[287] Comprehensive privacy legislation was the most common type of bill, introduced in at least 25 states. Comprehensive legislative is defined here as similar to the CCPA, i.e., broadly regulating the collection, use and disclosure of personal information and providing an express set of consumer rights with regard to collected data, such as the right to access, correct and delete personal information collected by businesses. *2021 Consumer Data Privacy Legislation*, National Conference of State Legislatures (December 27, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx.

[288] Jordan Yallen, "UNTANGLING THE PRIVACY LAW WEB: WHY THE CALIFORNIA CONSUMER PRIVACY ACT FURTHERS THE NEED FOR FEDERAL PREEMPTIVE LEGISLATION," Article, *Loyola of Los Angeles Law Review* 53, no. 4 (2020). Pg.

[289] "CCPA-/CPRA-Related Legislation Tracker," updated October 10, 2022, accessed October 1, 2022, https://iapp.org/resources/article/ccpa-cpra-related-legislation-tracker/.

[290] For a detailed account of corporate and privacy activist lobbying efforts, see Issie Lapowsky, "Inside the closed-door campaigns to rewrite California privacy law, again: How Google, Facebook, the EFF and others lobbied Alastair Mactaggart — and what they managed to get," *Protocol* (February 6, 2020). https://www.protocol.com/inside-california-privacy-law-redo.

redress that will render Facebook's liability-limiting statements discussed earlier in this case study. It also creates a dedicated, independent California data protection authority. The law was passed through state referendum with a 56 percent "yes" vote to expand privacy protections for consumers and thus gave the legislation strong democratic legitimacy.[291] The close adoption of GDPR standards spawned at least one news article addressing whether the US legal system would allow California to attain adequacy status as an independent territory.[292]

Table 3 shows the five states that have passed comprehensive legislation in line with the GDPR and the qualifications of their adoption. Of these, California is still widely considered to be the strongest benchmark for consumer protection. While the other four states do check the GDPR boxes, they include provisions and limitations that do not quite rise to the level of protections extended by California. Besides those five states, an additional five have active consumer privacy legislation proposed.[293] Legal scholar Daniel Solove identifies the movement at the state level as one of the causal factors behind Congress's newly proposed American Data Privacy Protection Act. "The sand grains spawning the federal pearl are the recent state consumer privacy laws. Starting in 2018, California passed the California Consumer Privacy Act (CCPA). Other states followed suit, such as Virginia, Colorado, Connecticut, and Utah. These laws aren't that

[291] "2020 California Proposition 24 - Expand Consumer Privacy Election Results," *USA Today* (November 3, 2020). https://www.usatoday.com/elections/results/race/2020-11-03-ballot_initiative-CA-8801/.
[292] See, for example, Andrei Gribakov, "Road to Adequacy: Can California Apply under the GDPR?," *Lawfareblog.com*, 2019, https://www.lawfareblog.com/road-adequacy-can-california-apply-under-gdpr. California adequacy status would be unlikely for nuanced constitutional reasons described in this essay.
[293] IAPP, "CCPA-/CPRA-Related Legislation Tracker."

great…, with California being by far the best of a rather mediocre bunch. But the states are moving rapidly. And these laws can grow and evolve," notes Solove.[294]

The California initiative—cemented through a public referendum—endangers the ideological commitment to fragmented regulation and weak government identified by Matthijs and Parsons. This opposition is ironically driving federal level corporate lobbying that aims to preempt state action. The federal initiative is the topic of the next section.

[294] Daniel Solove, "A Faustian Bargain: Is Preemption Too High a Price for a Federal Privacy Law?," Daniel Solove ed. *Privacy & Security Blog*, July 22, 2022, https://teachprivacy.com/a-faustian-bargain-is-preemption-too-high-a-price-for-a-federal-privacy-law/.

US State Comprehensive Consumer Privacy Bills Passed															
			CONSUMER RIGHTS								BUSINESS OBLIGATIONS				
STATE	**BILL NAME** (passed)	**EFFECTIVE DATE**	Right of access	Right of rectification	Right of deletion	Right of restriction	Right of portability	Right to opt out of sales	Right against automated decision making	Private right of action	Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments	Prohibition on discrimination (exercising rights)	Purpose/processing limitation
California	California Consumer Privacy Act (2018)	2020	X		X		X	X		limited	age 16	X			X
	California Privacy Rights Act (2020)	2023	X	X	X	sensitive data	X	X	X	limited	age 16	X	X	X	X
Colorado	Colorado Privacy Act (2021)	2023	X	X	X	opt out for targeted ads	X	X	opt out		sensitive data, age 13	X	X	X	X
Connecticut	An Act Concerning Personal Data Privacy and Online	2023	X	X	X	opt out for targeted ads	X	X	opt out		age 16	X	X	X	X
Virginia	Virginia Consumer Data Protection Act (2021)	2023	X	X	X	opt out for targeted ads	X	X	opt out		sensitive data, age 13	X	X	X	X
Utah	Utah Consumer Privacy Act (2022)	2023	X		X	opt out for targeted ads	X	X			age 13	X		X	
	source: IAPP		X = right exists												

TABLE 3: US STATE COMPREHENSIVE CONSUMER PRIVACY BILLS PASSED

5.9 Congress Responds: American Data Privacy and Protection Act

> *"The US is not in the driver's seat on this. The EU is…and we have to stop thinking that this [legislation] is just for Americans. So, Congress should put forth a bill that at least would put us on the global stage." – Jody Westby, global cyber risk advisor, commenting on the proposed American Data Privacy and Protection Act* [295]

Data governance initiatives in the US federal executive branch and states have collectively created greater pressure for the US Congress to act decisively. This is consistent with the prediction of the NIA's cross-national layering, whereby external international pressures can be transmitted through domestic channels. Besides the states, Congress has proposed approximately 17 federal consumer privacy bills. In keeping with the U.S. preference for sectoral regulation, there are yet other bills proposed to protect privacy at the sectoral level. However, because of their alarm over California's law and the action it inspired in other states, corporates actively started to lobby for a national level law that would specifically preempt the right of the states to enact legislation.[296] The result was a proposed federal law released in draft form on June 3, 2022. The *American Data Privacy and Protection Act* is the first bicameral and bipartisan proposal to come out of Congress in the decade since the privacy debate assumed greater urgency. The importance of the proposed comprehensive bill is not whether it passes but the degree to which it has incorporated GDPR conceptions of data privacy and protection. Like China's PIPL, the proposed legislation does not include all the features of the GDPR, but it would

[295] Daniel Solove, "A Federal Comprehensive Privacy Law: A Discussion of the ADPPA." https://teachprivacy.com/webinar-federal-comprehensive-privacy-law-access/.
[296] Jessica Guyunn, "Amazon, AT&T, Google push Congress to pass online privacy bill to preempt stronger California law," *USA Today* (September 26, 018). https://www.usatoday.com/story/tech/news/2018/09/26/amazon-att-google-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002/.

represent a substantial move in the direction of European-style privacy regulations. It has received a surprisingly high level of civil society support, including positive comments from various advocacy organizations, including the Future of Privacy Forum, EPIC, and the 21st Century Privacy Advocates. A survey by Morning Consult found that 80% of voters surveyed favored key provisions of the proposed legislation.[297]

One privacy advocate described the proposed bill as "the first significant, nationwide expansion of civil rights protections in over a decade."[298] The introduction of civil rights language mirrors the TADA and is a step beyond the language used in the California legislation. Like the California legislation, the ADPPA introduces the eight new rights present in the GDPR. Key features that reflect the hallmark GDPR language and important legal ideas include: protections for sensitive data; rights to access and correction; right of relief through the courts; a (somewhat) independent data authority; restrictions on how data can be processed; some requirements for explicit consent from data subjects (data minimization), among others. Another feature not represented in the California bill is the requirement for privacy by design, i.e., setting privacy defaults to the most stringent settings. Legal scholars and privacy activists have argued that the bill provides even more comprehensive protections than California's CPRA, even as it falls short of the GDPR in some respects.[299] Importantly, the bill includes language requiring *necessity and proportionality,* concepts that were also introduced in the TADA.

---

[297] *National Tracking Poll #2206078 Crosstabulation Results*, Morning Consult + Politico (June 10-12, 2022), https://assets.morningconsult.com/wp-uploads/2022/06/14130054/2206078_crosstabs_POLITICO_RVs_v1_06-15-22_SH.pdf. Pgs. 167-186.

[298] Bertram Lee, "Federal privacy legislation that protects civil rights is critical for all Americans," *The Hill* (July 21, 2022). https://thehill.com/opinion/congress-blog/3568525-federal-privacy-legislation-that-protects-civil-rights-is-critical-for-all-americans/.

[299] Solove, "A Federal Comprehensive Privacy Law: A Discussion of the ADPPA."

While the draft bill explicitly allows individuals the right to obtain relief in the courts for violations of privacy—a key condition for adequacy—, it still defends the existing institutions. Under the bill's terms, the FTC has the first right to bring cases against violators for four years after the ADPPA takes effect. Only then will private plaintiffs be able to bring claims for compensatory damages. Plaintiffs would be required to notify the FTC and state attorneys general prior to filing such suits, and actions for relief would be subject to a 45-day period in which federal and state authorities could respond to the notification. This construction was a compromise between lawmakers opposed to potentially frivolous lawsuits and lawmakers who argue that the enforcement exclusively by regulators is subject to lack of resources and regulatory capture. Still, the FTC would be granted broad rule-making powers and discretion to allow them to become an effective enforcer of the law. In other words, the United States would have an institution with the power to act as the equivalent of an independent data protection authority.

5.9.1 Preemption

The bill differs meaningfully from the GDPR in its preemption clause. Within the EU, the GDPR functions as a regulation that sets a minimum bar. EU members are permitted stricter data privacy and protection criteria, as long as they do not conflict with key features such as the mandate to limit data localization requirements.[300] Indeed some states like Germany do have stronger protections than that of the EU. One of the useful functions of this feature is that individual member states can address problems that arise as the regulation is interpreted and enforced by the courts and regulatory agencies. Member states both serve as areas for

[300] "EU to ban data localisation restrictions as ambassadors approve deal on free flow of data," news release, June 20, 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/eu-to-ban-data-localisation-restrictions-as-ambassadors-approve-deal-on-free-flow-of-data/.

experimental innovation, ensuring that the law remains active and preventing it from becoming a victim of legal torpor. In the United States, state "laboratories" of privacy regulation have contributed many legal innovations such as data breach notification law, requirements to provide people with free credit reports, and requirements to allow people to freeze their credit, among others.[301] More importantly, should the federal law become outdated, states can *de facto* step in to update legislation should Congress fail to act.

As written, the ADPPA would preempt state level consumer data privacy laws. Social media and other large firms have argued for preemption on the grounds that it will reduce compliance costs across state lines. California has resisted these efforts, as might other states who prefer the option to impose stricter requirements. Many privacy activists have argued that deviating from the GDPR in this way does an end-run around some of the more rigid requirements that favor consumers. In short, "preemption seems to be the Faustian bargain behind any federal privacy law today. After resisting a federal privacy law for years, industry now wants one because it fears that the innovations being concocted in the various state legislative laboratories," says Daniel Solove.[302] Whatever the outcome of these deliberations, European data governance preferences now play a dominant role in the American debate.

5.10 Conclusion

This chapter has shown how the NIA and the Brussels Effect were both at work in promoting European data governance preferences to the United States. In the US case, the GDPR

[301] Paul M. Schwartz, "Preemption and Privacy " *Yale Law Journal* UC Berkeley Public Law Research Paper No. 1404082 (2009), https://ssrn.com/abstract=1404082

[302]Solove A Faustian Bargain: Is Preemption Too High a Price for a Federal Privacy Law?

specifically forced the adoption of European rules overturning long-standing US resistance to the generalized global convergence on more comprehensive and prescriptive data governance. The US case at the federal level empirically fits with what is predicted by the NIA. The passage of the GDPR and the strong defense of it through the European Court of Justice shows how the change in European data regulation opened the window for a new set of transnational actors to defend and extend European preferences. Through the European Court of Justice, privacy advocates now have meaningful veto power over EU-US data transfer agreements.

However, the evidence also shows that the Brussels Effect influenced the current debate on privacy regulation in the United States. Corporates with exceptional market power have implemented European data privacy policies across their global platform. States with important economic power, such as California, have also voluntarily adopted European data privacy laws that reflect the human rights spirit of the GDPR, even as they fall short of using the language of human rights. Through the voluntary adoption of European-style data privacy rules, states pressured Congress to act decisively on comprehensive data transfer legislation. This pressure resulted in the proposed ADPPA. Alongside states, corporations have played an important role in influencing the contents of that proposed legislation, seeking to force a national standard that would harmonize regulation across all 50 states.

Meanwhile, since the Schrems II ruling, noyb has continued its active pursuit of GDPR enforcement on behalf of EU citizens. In total, noyb has filed complaints against 101 companies to challenge GDPR enforcement and generate legal precedents that can be used in subsequent cases. In the complaint, Schrems argued that the 101 companies that use Google analytics tools

transfer customer data to Google.[303] Since the US Cloud Act governs Google, US government authorities can request access to the customer information of these European companies through Google's cloud servers, even if they are located outside the United States. Thus, in a January 2022 decision, the Austrian Data Protection Authority ruled that the continuous use of Google Analytics violates the GDPR.[304] US firms will undoubtedly continue to be targets of legal challenges from the EU. As the EU strives for some version of data sovereignty, its regulatory influence will extend far beyond personally identifiable information.

[303] The US Cloud Act of 2018 gives U.S. law enforcement authorities the power to request data stored by most major cloud providers, even if it is outside the United States.
[304] "Austrian DSB: EU-US data transfer to Google Analytics," noyb, updated January 13, 2022, accessed August 1, 2022, https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal.

6 Chapter VI: Japan & EU Adequacy Status

6.1 Introduction

When the EU and Japan struck the Strategic Partnership Agreement (SPA), the Economic Partnership Agreement (EPA), and the data transfer adequacy agreement in succession, it was a monumental event. The EPA created the world's largest economic trading block covering 630 million people. On the day the EPA deal was signed, European Commission President Jean-Claude Juncker also announced the conclusion of adequacy status negotiations, indicating how closely intertwined the three deals were. Yet, the events barely drew global headlines because they did not involved China or the United States.

This chapter frames the Japan case in the geopolitical context surrounding its adoption of European data privacy conventions and shows how strategic imperatives created an aperture for the EU to bring Japan closer to its data privacy preferences. China's increasingly aggressive foreign policy toward Japan, coupled with the US's withdrawal from the Trans-Pacific Partnership (TPP) and its general retreat from leadership in multilateral fora, raised the salience for both the EU and Japan to cooperate on trade and data flows. Borrowing a framework from Julie Gilson, the adequacy story between the EU and Japan encompasses the following features: 1) agents, both Shinzo Abe and the redefined role of the European Parliament after the 2009 Treaty of Lisbon[305]; 2) institutions, including the long-established cooperation between the EU

[305] The Treaty of Lisbon granted the EU the authority to negotiate and sign treaties on behalf of all member nations. It also gave the EU Parliament the right to ratify trade treaties, which raised the stakes for negotiators to address key EU parliamentary concerns.

and Japan in multilateral organizations, and; 3) a changing context both domestically and regionally for each jurisdiction that motivated the EU and Japan to act when they did.[306]

Japan became the first Asian nation to attain adequacy, representing a breakthrough for European aspirations to extend their global data governance preferences to Asia. Japanese Prime Minister Shinzo Abe played a clinching leadership role in his broader grand strategy for transforming Japan into a "normal" international actor. His leadership was supported by the long-standing dialogue that had created an environment of trust between the two interlocutors. Like the US, Japan never embedded the human rights language into its data privacy regime, but the legal changes it made took a major step to protect personally identifiable information in ways consistent with the EU value-based approach. The EU did not have a trade relationship with Japan significant enough to afford it traditional market power leverage in adequacy negotiations. In 2019, the EU exported €94 billion in goods and services to Japan while imported €79 billion in kind from Japan. The EU exported roughly 2 ½ times that to China and imported more than 4 times that from China.[307] Thus, it was the confluence of strategic and economic interests that generated the logic for an adequacy finding.

The dynamics of the Japan case cannot be fully understood through the lens of the Brussels Effect or the NIA. To be sure, Japan voluntarily adopted European data governance rules, and it did so with the express intention of attaining adequacy status with the EU as would be predicted by the Brussels Effect. However, it did not do so independently of its relationship

[306] Julie Gilson, *EU-Japan relations and the crisis of multilateralism* (London and New York: Routledge, 2020). https://www.taylorfrancis.com/books/9780429326134. Pg. 10. For an excellent literature review of theoretical approaches to the EU-Japan relationship, cf. Gilson (2020) Chapter 1.
[307] https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan_en

with the EU. Shinzo Abe's administration successfully sought to link EU-Japan trade negotiations to a data transfer arrangement, something the EU had resisted.[308] Moreover, while Japan largely deferred to the European Commission's request for better EU citizen data rights under Japanese law, it was able to secure an important concession that these additional requirements initially be met through soft law mechanisms rather than through legislative change. To the degree that EU negotiators demurred, the dynamic bears the iterative feature of the NIA. However, the EU-Japan adequacy agreement did not garner much attention from civil society actors who might have opposed it, nor did it bear the NIA hallmarks of cross-national layering. The agreement remained largely driven by the Commission and Japanese counterparts rather than NGOs, privacy and human rights activists, and even the European Parliament. These features made it very different—almost opposite—from the U.S. case, perhaps highlighting just how scant attention Europe traditionally paid attention to Asia ex-China.

This chapter unfolds as follows. First, it provides an overview of the literature written on the Japan adequacy case. Second, it briefly reviews the evolution of the EU-Japan relationship over the decades. It then provides the broader context into which Shinzo Abe arrived on the international stage and shows why Abe's role in strategic and economic partnership negotiations was also critical to realizing the data transfer agreement. Next, it reviews details of the adequacy negotiations highlighting Japan's legal changes to accommodate EU requirements and their implications. The agreement details showcase a high degree of policy entrepreneurship from the Japanese side. Finally, it concludes with a discussion of what has occurred since the

[308] Elaine Fahey, *The EU as Global Digital Actor*, Modern Studies in European Law, (Oxford: Hart Publishing, 2022). Pp. 152

adequacy finding was first struck and what the arc of the narrative it tells us about the Brussels Effect and the NIA.

6.2 Literature Review

Authors who have previously considered the Japan data adequacy case include Paul M. Schwartz, Flora Wang, and Suda Yuko. Each author looks at the EU-Japan adequacy negotiations and describes the changes Japan made to its laws in service of the arrangement. They do not seek a causal framework per se. This chapter layers onto the findings of these three authors, the element of Japan-EU geopolitical considerations and trade negotiations as an explanatory variable for why Japan would reform its data protection framework to reflect EU policy preferences.

Consistent with the adequacy model analysis herein, Paul M. Schwartz challenges the applicability of the Brussels Effect to the Japan case. Instead, Schwartz suggests that there is a "varied range of nation-state, transnational, and corporate behavior that has helped spread EU data protection throughout the world."[309] While "the EU's adequacy requirement has provided the EU with important negotiating leverage," the Japan and the U.S. case studies "demonstrate that the EU's regulatory capacity arises from a complex interplay among EU institutions and outside influences, rather than the EU exercising power as a monolithic entity."

Schwartz traces the timeline of negotiations and suggests that, by linking trade and data privacy protection, the EU-Japan agreement demonstrates "a new model for reconciling international trade law and data protection law."[310] Some authors have suggested that the EU's

[309] Schwartz, "GLOBAL DATA PRIVACY: THE EU WAY." Pg. 773-774.
[310] Ibid, pg. 790.

GDPR might be interpreted as protectionist and could therefore subject it to scrutiny under the WTO.[311] The EU-Japan agreement suggests a solution to the potential protectionist challenge, a consideration that may have contributed to incentivizing policy makers to pursue the new model.

Flora Wang traces the story of Japan's adequacy finding through interviews in Tokyo, describing it as "cooperative data privacy." She shows that "in contrast to Europe, the Japanese privacy framework emphasizes the importance of data as an economic commodity and protects a narrower range of personal information. Article 13 of the Japanese Constitution and subsequent tort case law implicitly recognize the right to privacy. However, Article 13 of the Japanese Constitution strikes a very different tone from the European *Charter*, unlike the latter, it omits any explicit references to the right of privacy or data protection."[312] Wang goes on to demonstrate how Japan and the EU finessed the differences in cultural attitudes toward data privacy in their agreement. She also highlights the growing internal tension between Japanese multinationals and domestic firms with differing objectives, a dichotomy that also emerged in the UK-EU adequacy talks after Brexit.[313]

Yuko Suda argues that Japan yielded to the EU's substantial demands for legal reform in data protection and documents the areas of concession. She attributes the change in Japan's domestic data protection regime to the extraterritorial effect of the EU's laws, whose privacy

[311] Yakovleva, "Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade 'Deals'?."
[312] Flora Y. Wang, "COOPERATIVE DATA PRIVACY: THE JAPANESE MODEL OF DATA PRIVACY AND THE EU-JAPAN GDPR ADEQUACY AGREEMENT," Article, *Harvard Journal of Law & Technology* 33, no. 2 (Spring2020 2020). Pg. 669.
[313] Bruno Gencarelli, "In Conversation With Mr. Gencarelli, The EU's Head of International Transfers," interview by Lore Leitner, *IAPP Europe Data Protection Congress*, November 17, 2021.

provisions with growing citizen concern for data privacy.[314] She also notes that Japan's shift is consistent with the long-standing view among international relations scholars that internal changes are often a result of external or foreign influences, for example in the work of Kent E. Calder.[315] However, Suda's argument is not entirely consistent with the activism of the Shinzo Abe administration, whose signature foreign policy initiative was to transform Japan into a normal international actor.[316] In doing so, Japan is increasingly shedding the image that it responds first and foremost to external influences.

6.3 The Long Arc of EU-Japan Relations

Julie Gilson elegantly documents the long and gradual institutionalization of the EU-Japan relationship. "Relations [between the EU and Japan] have been shaped by actor characteristics, institutional dynamics and contextual constraints and opportunities," she writes.[317] In the immediate aftermath of WWII, both sides focused on economic rebuilding and operated under the dominant influence of the U.S. security umbrella. Due to its role in WWII, Japan played no role in forming regional frameworks from the end of the war through the 1970s, while the European Community simultaneously focused on the institutionalization of the Single Market.

An EU-Japan partnership was established through the Joint Declaration in 1991 and became one of many soft law instruments that dominated the relationship until the 2001 Action

[314] Suda Yuko, "Japan's Personal Information Protection Policy Under Pressure: The Japan-EU Data Transfer Dialogue and Beyond," Article, *Asian Survey* 60, no. 3 (2020), https://doi.org/10.1525/AS.2020.60.3.510.
[315] Kent E. Calder, "Japanese Foreign Economic Policy Formation: Explaining the Reactive State " *World Politics* 40 (4) (1988).
[316] Gilson, *EU-Japan relations and the crisis of multilateralism*. Pg. 5.
[317] Ibid, Pg. 10.

Plan. With that Plan, interactions became more earnest. It laid out an ambitious agenda that ultimately did not yield any trade or cooperation agreements but rather opened the door to an ongoing dialogue. The informal structure enabled a mutual learning process to build trust and start to untangle some major regulatory, institutional, and cultural barriers to trade.[318] In the post-Cold War era, both the EU as a cohesive entity and Japan as the world's second largest economy gradually emerged on the global stage as rising international actors. Thus, it represented both sides' interests to initiate committed intergovernmental discussions. Yet despite the mutual interest in further cooperation, Japan and the EU were overwhelmed by internal politics and the foreign policy priorities dictated by their respective relationships with China and the United States.[319]

The Action Plan came in tandem with Japan's first major post-WWII trade agreement with Singapore in 2001, the Japan-Singapore Economic Agreement for a New Age Partnership (JSEPA), which set in motion a new era of trade engagement with the region for Japan. In doing so, Japan was joining a trend of PTAs and FTAs that was already well-established among other global players but which had met with considerable domestic resistance.[320] That same year, China joined the WTO with the support of both the EU and Japan, firmly establishing its place in the international trade order.

When the ten-year Action Plan ended, the two sides agreed on the need to renew talks and drive toward more concrete outcomes. Yet, there was no real catalyst to move them

[318] Fahey, *The EU as Global Digital Actor*. Pg. 148.
[319] Gilson, *EU-Japan relations and the crisis of multilateralism*. Pg. 103.
[320] Mark Manger, "Competition and Bilateralism in Trade Policy: The Case of Japan's Free Trade Agreements," *Review of International Political Economy* 12, no. 5 (2005), https://doi.org/http://www.tandfonline.com/loi/rrip20.

forward. Throughout this engagement, the EU and Japan held divergent views on China. While the EU clung to the aspiration that trade could bring China to evolve into a more liberal democratic order under the moniker of *Wandel durch Handel*, Japan clearly perceived China as not only a rising power but as one that did not embrace the status quo.[321] Japan saw China as a challenger to the liberal international order. Over time, the EU would draw closer to Japan in its viewpoint on China. Shinzo Abe was an important figure in this transformation. When Abe became prime minister for the second time in 2012, the EU-Japan relationship found the catalytic leadership it needed. On the other hand, Abe benefitted from the mutual trust built over the past two decades and could leverage that trust to affect change.

6.4 Shinzo Abe Transforms Japan

> *"Xi Jinping made Abe... [he] should never have come back politically. He came back because he studied strategy….and China began bullying all of its maritime neighbors, especially Japan…. The 2012 Senkaku crisis….created a consensus in [the ruling party], 'We need to bring Abe back. He's the guy who can stand up to China.' " -- Michael Green, Japan scholar, Center for Strategic & International Studies*[322]

Shinzo Abe rose to power on an unabashed nationalist agenda largely responsible for a realist articulation of Japanese foreign policy vis-à-vis China. The realist posture remains an important feature of Japan's diplomacy even after Abe's resignation in 2020 and assassination in 2022.[323] Called again to lead in 2012, he arrived on the scene with a mission: 1) to sweep aside Japan's WWII legacy as a dominating shaper in its foreign policy; 2) to adjust its relationship

[321] *ChinaPower*, podcast audio, The State of Japan-China Relations: A Conversation with Christopher Johnstone, https://chinapower.csis.org/podcasts/the-state-of-japan-china-relations/.
[322] Michael Green, *The Asia Chess Board*, podcast audio, The Legacy of Shinzo Abe, 2022. At section 8:35.
[323] Michael Auslin, "Japan's New Realism," *Foreign Affairs* March/April 2016, https://www.foreignaffairs.com/articles/japan/2016-02-16/japans-new-realism.

with the United States by transforming itself into a regional security partner rather than a nation under the U.S.'s security umbrella; 3) to extract Japan from a decade of failing economic policy, and; 4) to alter the strategic environment around China to disincentivize its aggressive posture in the South China Sea and towards its Asian trading partners.

To do this, he not only created a grand strategy for Japan, but he also articulated policies whose language became part of mainstream global diplomatic parlance. Among them was the concept of the "Free and Open Indopacific," a term later adopted by the EU and by the United States. The U.S. Defense Department switched the name of its top military command in the region from U.S. Pacific Command to U.S. Indo-Pacific Command in 2018, a testament to Abe's influence.[324] In particular because of multiple confrontations with China over the Senkaku Islands, Abe revitalized the U.S.-Japan security alliance by expanding the parameters for Japan's contributions. He spearheaded legislation allowing Japan's military to exercise collective self-defense and increase military spending to nearly 2 percent of GDP from less than 1 percent.[325] Abe also revived the QUAD, a proto-alliance including Australia, India, and the United States, that he had inaugurated during his first time as Prime Minister in 2006 meant to signal a security counterbalance to China.

One of his signature achievements was making EU-Japan relations a mainstream feature of Japan's foreign policy, when it had previously been subordinate to US and China relations. "Strengthening strategic partnerships with Europe [is] one of the most tangible achievements

[324] Jack Detsch, "Abe's Legacy Will Outlive Him," (July 8, 2022). https://foreignpolicy.com/2022/07/08/shinzo-abe-assassination-japan-indo-pacific-security/.
[325] Ibid.

of Prime Minister Abe Shinzo's foreign policy.… Abe understood the importance of Europe for Japan and, most crucially, what he tried to do … was to mainstream relations with Europe within Japan's overall foreign policy. In the past, relations with Europe were often seen as somehow detached from Japan's vital national interest. Abe, instead, tried to get Europe on board in addressing regional and global issues vital for Japan," notes Keio University Professor Michito Tsuruoka.[326]

As H.D.P. Envall has observed, through "Japan's Indo-Pacific diplomacy, the Abe administration has pursued the idea of engaging more with the region as a major policy prescription, not only with a view to buttressing America's position in Asia, but also to support what it views as the region's 'liberal international order'…. the government views the protection of this order 'based on rules and universal values' as in Japan's 'national interests.' The Abe administration's prescriptions for regional diplomacy, therefore, mix a type of values-based rhetoric with a realist counterbalancing logic."[327] This values-based rhetoric is not just in its diplomatic language but is present in its first national security strategy. Initiated at Abe's request, Japan's 2013 security strategy links its national interests to upholding "universal values, such as freedom, democracy, respect for fundamental human rights and the rule of law."[328]

This new and clear articulation of Japan's aspirations harmonized with the European values emphasized in the EU's signature documents. The EU and Japan pursued what today are known as the Strategic Partnership Agreement and the Economic Partnership Agreement

[326] Michito Tsuruoka, "Abe Shinzo's Legacy in Japan-Europe Relations," *The Diplomat*, September 14, 2020, https://thediplomat.com/2020/09/shinzo-abes-legacy-in-japan-europe-relations/.
[327] H.D.P. Envall, "The 'Abe Doctrine': Japan's new regional realism," *International Relations of the Asia-Pacific* 20, (2020) 31–59 (2018), https://doi.org/10.1093/irap/lcy014.
[328] GOJ and Government of Japan, National Security Strategy, (2013).

against this backdrop. While the EU had already pursued strategic partnerships in tandem with economic agreements, this would be the first time Japan ever followed such a model. In normative terms, the Strategic Partnership Agreement addressed wide-ranging issues, including arms control, climate change, malign finance, and the law of the sea. It also reflected a strategic focus on data flows. The final document of the Strategic Partnership Agreement included references to privacy and personal data protection in Article 8 (counter-terrorism), Article 37 (passenger name records), and Article 39 (general personal data protection).[329] Article 36 highlights the importance of ensuring global data flows

> *"The Parties shall enhance cooperation in order to promote and protect human rights and free flow of information to the maximum extent possible in cyberspace. For this purpose, and based on the understanding that international law applies in cyberspace, they shall cooperate, where appropriate, in establishing and developing international norms and promoting confidence building in cyberspace."*[330]

In the context of Abe's grand strategy, the SPA was not just another in the series of dialogues between the EU and Japan. It was the platform to launch the Economic Partnership and the data transfer agreements that meaningfully deepened EU-Japan ties.

6.4.1 Shinzo Abe and Japan's Trade Push

From an economic perspective, the Abe administration emphasized solidifying and expanding Japan's trade relations worldwide as part of his signature Abenomics.[331] After many years of resistance to joining TPP negotiations, Prime Minister Abe not only joined the talks in

[329] Strategic Partnership Agreement between the European Union and its Member States, of the one part, and Japan, of the other part, (2019).
[330] Ibid, pg. 29.
[331] Mireya Solis and Shujiro Urata, "Abenomics and Japan's Trade Policy in a New Era," *Asian Economic Policy Review* 13 (2018).

2013 but later played a vital role in negotiations. During Abe's tenure, Japan's traded goods that resulted from trade agreements went to 85% from 17% of total trade volumes.[332] In 2000, Japan's exports represented 22% of its economic output, and Europe's exports represented 35.7% of its aggregate economic output. Two decades later, when the EPA was inked, Japan's exports were 29% of its GDP and the EU's exports represented 49% of EU GDP.[333]

Previous Japanese administrations had first sought trade talks with the EU in 2010. In response, formal negotiations began in 2013 and were conducted over 18 rounds. The talks were slowed for a considerable period when the EU faced difficulty getting Japan to take action on non-tariff barriers. In addition, both the EU and Japan were actively engaged in other trade agreements that affected their strategic logic in dealing with one another. Japan was negotiating the TPP while Europe was negotiating a bilateral agreement with Korea. Any concessions each party made in those agreements might force them to make similar concessions in an EU-Japan trade agreement. When the EU-Korea and TPP negotiations concluded, Japan and the EU had an opening to accelerate their discussions.[334]

The immediate cause for the EU and Japan to reinvigorate their trade talks was US president Trump's withdrawal from the TPP. Shinzo Abe surprised his domestic audience when he took active steps not only to save the TPP but also to preserve the ability of the United States to rejoin the TPP if US leadership changed in 2020. For its part, the EU was motivated to act

[332] Cf. Michael Green, *The Asia Chess Board*, podcast audio, The Asia Shogi-board: Strategic Insights with Yoichi Funabashi, 2021. See also Michael Green, "Shinzo Abe's Decision to Step Down," *Critical Questions*, *Center for Strategic and International Studies*, 2020, https://www.csis.org/analysis/shinzo-abes-decision-step-down.
[333] https://data.worldbank.org/indicator/NE.EXP.GNFS.ZS?locations=EU
[334] Hidetaka Yoshimatsu, "The EU-Japan Free Trade Agreement in Evolving Global Trade Politics," *Asia Europe Journal* 18, no. 4 (2020). Pgs. 432-433.

quickly for fear of losing out to the countries that remained in the new TPP.[335] From Japan's side, it was concerned about losing out to Korea because of the EU-Korea free trade agreement.[336] Japan had seen its automobile exports to the EU fall, while Korean exports to the EU increased after the conclusion of the EU-Korea trade deal. Similarly, Japanese exports covered by the Korea-EU agreement fell while EU exports shot up by 15.4%.[337] When the talks were relaunched, the EU-Japan Economic Partnership was one of the most swiftly concluded trade agreements since the EU launched its "Global Europe" initiative in 2006.[338]

6.4.2 Linking Data and Trade

Establishing a well-defined link between trade and data flows appears to be a logical path for policymakers. But such an approach has eluded them since the beginning of the internet. Susan Aaronson has argued that negotiators have not "been able to use trade negotiations to set information free" for several reasons.[339] First, the international community is still debating which information flows are traded services and whether trade agreements can properly regulate data flows. Second, policymakers in the US and EU did not effectively link efforts to promote the free flow of information with efforts to promote digital rights and internet freedom. Finally, Aaronson highlights that early disagreements between many countries on these issues led the United States to retreat from a leadership role in the cross-border data flow debate. Thus, "policymakers have not found common ground in international agreements designed to

[335] The revived version, the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) was concluded in Tokyo in 2018 and included 11 countries: Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam.
[336] Gilson, *EU-Japan relations and the crisis of multilateralism*. Pg. 115.
[337] Yoshimatsu, "The EU-Japan Free Trade Agreement in Evolving Global Trade Politics." Pg. 434.
[338] "Global Europe: Competing in the world," in *European Encyclopedia of Law*. https://europeanlaw.lawlegal.eu/global-europe-competing-in-the-world/.
[339] Susan Aaronson, "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security," *World Trade Review* 14, no. 4 (2015).

explicitly facilitate information flows, but they have established human rights language to guide these flows."[340] Through their economic, strategic, and adequacy agreements, Japan and the EU were able to link and address the complex issues highlighted by Aaronson. That they did so despite the relatively weak trade flows between the two geographies highlights the broader geostrategic circumstances to which the EU and Japan were responding.

For Abe and his administration, data flows were inextricably tied to trade, and the foundation of the relationship with the EU was preserving the global trading order. He showed the inextricable link between data and trade in his thinking when he announced the Osaka Track initiative in 2019, through which he sought to drive consensus toward global rules for cross-border data transfers under the WTO umbrella. Through the TPP negotiations, Japan had already developed significant expertise in the complex nature of cross-border data sharing. The TPP negotiations contained multiple discussion rounds on digital commerce, resulting in the most comprehensive digital provisions to date when the agreement was concluded.[341] These provisions covered domestic electronic transactions, personal information protection, internet interconnection charge sharing, location of computing facilities, unsolicited electronic advertising, source codes, and dispute settlement. Importantly, the TPP also sought to restrict data localization measures that could serve as non-tariff trade barriers, a feature that would explicitly exclude China after its Cybersecurity Law was passed in 2016.[342] The digital provisions of the TPP

[340] Aaronson, "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security." Pg. 675. Note Aaronson's reference to human rights as a common language. While this is true at the multilateral level, this language is not commonly adopted at the national level in any of the three case studies of this thesis.
[341] Mira Burri, "The Regulation of Data Flows Through Trade Agreements," *Georgetown Journal of International Law* 48 (08/28 2017). Pg. 432.
[342] The TPP features a few exceptions to the ban on data localization, including finance services and government institutions.

remained in place in the CPTPP, the successor agreement that ensued after the United States withdrew from the TPP.

As a result, the Japanese proposed conducting trade and data transfer negotiations in parallel. The EU, however, resisted this link, in part because of internal bureaucratic competition between trade and data flow negotiators. The EU has a longstanding policy that the two should not be linked, despite a 2006 policy requiring each trade agreement to include sections on data flows.[343] Thus, there has always been a vast policy coordination gap between EU trade negotiators and data protection negotiators.[344] Because of its higher standards of data protection, the EU has written data protection clauses into its trade agreements to shield itself from action under the WTO GATS Article XIV. This clause is targeted against non-tariff barriers to trade. Some critics, including US negotiators, have argued at the EU's data protection laws function like non-tariff barriers. As a result, the EU has negotiated language in treaties to safeguard their right to legislate their data protection regime. The potential for conflict between data protection and trade law dates to WTO GATS but has only been discussed concretely since 2017, shortly after the GDPR was promulgated.[345] Here again, the GDPR's extraterritorial clause was a source of threat.

The EU ultimately conceded to Japan's suggestion, although it is unclear why they did. Certainly, many critics have argued that the EU did not sufficiently protect data rights under its

[343] Gencarelli, interview.
[344] Yakovleva, "Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade 'Deals'?."
[345] Anonymous, *Data Flows and Trade Agreements*, Open Rights Group (2021), https://www.openrightsgroup.org/publications/data-flows-and-trade-agreements/.

trade agreements.[346] Negotiating adequacy and trade in parallel talks served to blunt the data rights criticism and could facilitate European Parliament approval of the treaty. In addition, the EU's decision might have been influenced China's ever-more restrictive data governance, especially its Cybersecurity Law in 2016. Both Japan and the EU shared a common desire to prevent data localization. Many of Japan's multinationals operating in China had become ensnared in government crackdowns on cross-border data transfers. Japanese officials particularly cited the limits on data transfers outside of China as a barrier to efficient business.[347]

Thus, timing created the space for the EU to externalize its data governance framework in Asia through Japan. The sequential linkage of the three agreements was a policy innovation. While the EU had linked economic and strategic agreements in the past, Japan had not done so. For the EU, the comprehensive deal with Japan was the first executed in parallel data transfer negotiations.[348] In their joint press statement following the conclusion of discussions, chief negotiators Vera Jourova of the EC and Haruhi Kumazawa of Japan said,

> *"This decision will complement and enhance the benefits of the Economic Partnership Agreement and contribute to the strategic partnership between Japan and the EU. With this agreement, [Jourova and Kumazawa] reaffirm their commitment to shared values concerning the protection of personal data, and to strengthen their cooperation and demonstrate their leadership, in shaping global standards based on a high level of protection of personal data. The citizens of Japan and the EU will benefit from strong protection of their personal data while companies will benefit from the unhindered safe and free data transfers to each other's economies."*[349]

---

[346] Cf. Ante Wessels, "Broken data protection in EU trade agreements," *Foundation for Free Information Infrastructure*, https://ffii.org/broken-data-protection-in-eu-trade-agreements/.
[347] China's strict new cybersecurity law ensnares Japanese companies - Nikkei Asia
[348] Schwartz, "GLOBAL DATA PRIVACY: THE EU WAY." Pg. 17.
[349] PPC, Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, (2018).

6.5 EU Objectives

The EU could accomplish multiple policy objectives by pursuing multi-track negotiations that included trade and data flows with Japan. First, Japan's adequacy status would make it a powerful voice for EU data standards in a region that proved resistant to many of them. As of that time, no Asian nation had previously signed on to the even more minimal standards of the *Convention 108* despite the Council of Europe's push to internationalize the Convention's signatory base. While many nations did sign on to the APEC conventions, these standards fall far short of the GDPR's requirements and have not had a meaningful impact.

When Japan introduced the idea for mutual adequacy, or a mechanism through which both parties could recognize bi-directional data flows, it was welcomed by the EU as an unexpected innovation. Bruno Gencarelli, the chief EU data privacy negotiator, noted that the EU embraced the innovation in part as a means to further diffuse EU data privacy policy preferences throughout Asia.[350] Previous adequacy findings have addressed only the flow of data from the EU to other countries. Mutual adequacy meant that data-driven economic sectors in both Japan and the EU could benefit from lowered tariffs through the trade agreement.

In addition, given the EU's complex process of ratifying a trade treaty, gaining Japan's commitment to higher data privacy standards could make sticky trade concessions more palatable. Since the 2009 Treaty of Lisbon, trade agreements have required approval from the European Parliament. A famously vocal minority in the parliament has regularly threatened to use its veto power, often around issues relating to climate change or human rights. The EU's 2019 trade treaty with Mercosur, the South American customs union comprising Argentina, Brazil,

[350] Bruno Gencarelli comments at IAPP Data Congress, Brussels, November 2021.

Paraguay, and Uruguay, is one important example. While heralded at the time as a major achievement, the EU Parliament failed to ratify the deal with the South American customs union because of concerns by Green Party and environmental groups.[351] A year earlier, the EU parliament's 2018 report on climate diplomacy stated that approval of trade agreements is conditional on implementation of the Paris Agreement on climate change. When Brazilian President Jair Bolsonaro fulfilled his election promise to open millions of acres of ancient Amazon forest to more farming, the EU-Mercosur trade treaty all but died.[352]

While Japan had long cooperated with the EU on climate change issues, EU members of parliament were well aware of its shortcomings in data privacy protection. EU negotiators had an incentive to align the EU-Japan trade agreement with data adequacy status. In doing so, EU trade negotiators could harmonize the aspirational view that a human rights-based data privacy approach goes hand in hand with economic prosperity. The prospect of mutual adequacy was an added inducement for the European Parliament as it considered ratifying the EU-Japan trade pact that involved unpopular concessions.

6.6 From Illusion to Adequacy

Adequacy findings are the instrument through which the EU most vigorously promotes its data regulation preferences and the underlying human rights imperative. For Japan, achieving adequacy was a remarkable achievement given the considerable differences between the EU and Japan's data protection regimes. In a 2014 assessment of Asian data privacy laws,

[351] Bernd Lange, "EU-Mercosur: the Bolsonaro factor," *IPS* (May 3, 2019). https://www.ips-journal.eu/topics/foreign-and-security-policy/eu-mercosur-the-bolsonaro-factor-3296/.
[352] Gil Alessi, "The Amazon Rainforest under Bolsonaro: a story of fire and violence in Brazil," *El Pais USA*, English Edition (September 16, 2021). https://english.elpais.com/usa/2021-09-16/the-amazon-rainforest-under-bolsonaro-a-story-of-fire-and-violence-in-brazil.html. Brazilian presidential candidate Lula DaSilva has promised that if he wins in the next election, he would seek to revive the treaty with the EU.

Greenleaf characterized Japan as providing an "illusion of protection."[353] The transformation in a short period was profound.

6.6.1 Japan's Act on the Protection of Personal Information

In the 30 years prior to the adequacy agreement with the EU, Japan had evolved personal data protection rules that diverged from those of the EU. In 1988 the Act on the Protection of Personal Information Held by Administrative Organs (APPI) became Japan's first law that dealt with data privacy.[354] Unlike the GDPR, the Act was directed at government organizations and did not apply to the private sector, in keeping with Japan's desire to privilege economic development over individual privacy. In 1988, such an arrangement would have been acceptable to a domestic audience that—in the pre-internet era—did not share the same highly developed sensitivities to exposure of personally identifiable information.[355] It also reflected deference to the United States, which at the time was Japan's largest trading partner, not to mention its closest security ally in the region.

Increased globalization and the internal debate around Japan's national registration system (the *jukinet)* in 2002 raised awareness and motivated even those more passive about data privacy. During one public campaign against the launch of the pilot *jukinet* system, the Japanese newspaper *Asahi Shimbun* sponsored an opinion poll which showed that three-quarters of the population had doubts about the introduction of the system, citing concerns over the privacy and lack of confidence in the security of the system.[356] This debate contributed internally

[353] Greenleaf, *Asian Data Privacy Laws, Trade and Human Rights Perspective*.
[354] Kawabata 2016, pg. 264
[355] Andrew A. Adams, Yohko Orito, and Kioshi Murata, "The Japanese sense of information privacy," *AI & Society* (2009), https://doi.org/10.1007/s00146-009-0228-z.
[356] Adams, Orito, and Murata, "The Japanese sense of information privacy."

to Japan's impetus to update its Act on Protection of Personal Information (APPI) in 2003. The revised APPI reflected many of the original OECD principles and was thus in keeping with global trends. One outstanding feature was that the new law extended the scope of data protection to include businesses.[357]

Because it was written a decade before the GDPR, the 2003 APPI differed from the European standards in four key ways that were not unique to Japan. First, Japan did not have an independent data protection authority. This has been the case in many countries, including Brazil, China, and the United States. Second, it did not include provisions protecting sensitive information, such as religion or sexual orientation. Third, it did not contain provisions for individuals to obtain judicial relief in the case of data privacy infractions. Finally, the APPI did not address the cross-border transfer of personal data to a third country. In other words, EU citizen data that might be protected in Japan could be further sent on to another jurisdiction in which such protections would not be honored.[358]

The APPI was again updated in 2015 with intent to increase data flows among businesses to facilitate economic growth in the digital age. Recalling that trade negotiations between the EU and Japan had already started in 2013, Japan expressly revised its privacy laws in anticipation of seeking EU adequacy status. Yamaguchi Shunichi, the Minister in Charge of IT Policy, made public comments affirming Japan's aspiration for adequacy status.[359] The revised APPI addressed the EU's core requirements for an independent data protection authority and

[357] Yuko, "Japan's Personal Information Protection Policy Under Pressure: The Japan-EU Data Transfer Dialogue and Beyond.", pp. 514.
[358] China included these specifications most recently in its PIPL.
[359] Yuko, "Japan's Personal Information Protection Policy Under Pressure: The Japan-EU Data Transfer Dialogue and Beyond.", pp. 517.

the capacity for individual redress in the event of data privacy violations. It also included the right to rectification of incorrect information and the right to be forgotten.[360] It thus became the foundation for EU-Japan adequacy negotiations in 2017.

6.6.2 Adequacy Concessions

While the 2015 APPI accommodated most of the EU's core concerns, it also required further change. Because it passed one year before the passage of the GDPR, the authors of the revised APPI could not have anticipated all the new terms of the EU regulation. Japanese data protection regulators proposed to address the EU's concerns through guidelines (or supplemental rules) rather than reopening a complex legislative process, according to Suda.[361] Further changes to the formal law would be time-consuming and would undercut the goal of attaining adequacy in close sequential time with the trade agreement. For the EU, it was critical that the agreement would protect all of the rights of EU citizens, even if they did not extend the same protections to Japanese citizens. Without this protection, the adequacy finding would not stand up to scrutiny in the European Court of Justice.

Several issues posed stumbling blocks. One required Japan to broaden the definition of sensitive data. Another concern was the commitment by Japan to safeguard against the onward transfer of EU citizen data to jurisdictions that did not guarantee the same data protections as those in both the EU and Japan. Onward transfers would need to be certified by businesses and

[360] Cf. EU, Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Brussels 2019). EUR-Lex - 32019D0419 - EN - EUR-Lex (europa.eu)

[361] Yuko, "Japan's Personal Information Protection Policy Under Pressure: The Japan-EU Data Transfer Dialogue and Beyond." Pg. 520.

enforced by the Personal Information Protection Commission (PPC), Japan's independent data privacy enforcement agency.

Another European Commission requirement was that Japan establish a mechanism for EU citizen redress for violations of the law. To achieve the redress requirement and ensure rigor before the ECJ, Japan established a system through which EU citizens could lodge data privacy violation complaints. EU citizen cases can be filed with either the Japanese data protection authority via a binding decision and/or file a civil action to obtain damages or injunction with a Japanese court.

The Japanese proposed supplemental rules amending the 2015 APPI rather than legislation, which proved to be an additional sticking point for the Commission. European data privacy officials preferred "hard power" versus "soft power" enforcement, notes Wang. Japanese officials argued that reputational risk and the cost of losing consumer trust were a compelling incentive to make corporations comply. The PCC presented numerous cases in which reputational risk changed corporate behavior as evidence. By contrast, the Commission sought greater punitive measures against companies that did not comply with the APPI and the PPC supplemental rules. This push partly reflected the European Data Protection Board's resistance to "soft law" solutions in deals that would be subject to abuse by third countries.[362] After the EU's experience with the EU-US Safe Harbor agreement, the EU was particularly sensitive to introducing too many potential loopholes.

[362] For further discussion of soft law, see Fabien Terpan, "Soft law in the European Union ù the changing nature of EU law," Article, *European Law Journal* 21, no. 1 (01/01 / 2015).

Could the supplemental rules have been challenged in the European Court of Justice? They certainly might have been, and the court might have rejected the adequacy finding. The lack of challenge might be understood in terms of the differences between the U.S. case and Japan. The core complaint of Schrems I & II was that the private sector could share data with government officials without the knowledge or consent of the data subject. Such actions took place on a massive scale. Japanese companies do not engage in a fraction of the data gathering that American firms do, thus dramatically reducing the amount of data that might be transferred without authorization.

The EU ultimately deemed Japan's supplemental rules acceptable because they could be enforced through the independent data protection body, as noted in the EU's implementation document.[363] Moreover, Japan agreed to change its laws to bring them closer to the GDPR over time. The incentive to keep this promise is the periodic review conducted by the Commission. The next section details the legal changes Japan made since its adequacy finding.

6.6.3 Updates to the APPI

In 2021, Japan updated the APPI to better align with the GDPR.[364] The amendment expands the definition of sensitive information, extends greater access rights for data subjects, and allows businesses to use pseudonymized information internally, among other provisions. It also adds provisions regarding transfers of data to regions outside Japan. Firms will need to obtain an individual's opt-in consent prior to transferring that individual's personal information to a location outside of Japan or establish a personal information protection system with entities

[363] EC, COMMISSION IMPLEMENTING DECISION (EU) 2019/419, (Brussels: European Commission, 2019).
[364] Hiroyuki Tanaka, Naoto Obayashi, and Noboru Kitayama, "Analysis of Cabinet of Japan's approved bill to amend APPI," (March 18, 2021). https://iapp.org/news/a/analysis-of-japans-approved-bill-to-amend-the-appi/.

receiving the data in a foreign jurisdiction.[365] The additional changes show how the creation of institutions in Japan that represented EU data governance preferences did indeed have spillover effects that shifted Japan's conception of what is possible and desirable. That is, adequacy status came to shape and reflect what Japanese officials considered was in their national interests.

EU and Japan also conducted their first review of their adequacy agreement in 2021. In a joint press release, Didier Reynders, European Commissioner for Justice, said: "This review, by ensuring that our adequacy decisions work as intended, offers a unique opportunity to further strengthen our strategic partnership in this area both bilaterally and in multilateral fora." The language throughout the EU's announcements on data privacy consistently reinforces the linkage to the strategy and economic partnership agreements. From the Japanese side, Shuhei Ohshima, Japan's PPC Commissioner said: "We underline with the EU our joint commitment to high standards of protection for personal data, based on the already high degree of convergence between our systems. We also stress the importance of our continued cooperation on promoting 'Data Free Flow with Trust' globally."[366] Besides the shift in Japan's domestic laws after the initial adequacy finding, the launch of the *DFFT* initiative was one of the most notable results.

6.7 Conclusion

While the EU-Japan agreements barely got attention in the news cycle, the same was not true of the events that followed them. Shinzo Abe made headlines in June 2019 when he

[365] https://www.beneschlaw.com/resources/amended-japanese-privacy-law-creates-new-categories-of-regulated-personal-information-and-cross-border-transfer-requirements.html
[366] https://ec.europa.eu/newsroom/just/items/724795/en

proposed the "Osaka Track" on global data governance at the G20 meeting hosted by Japan that year.[367] With his proposal, Japan sought to assume a leadership mantle in facilitating the free flow of global data and halt the growing trend toward data localization that threatens international trade and economic growth. In his speech announcing the initiative at the World Economic Forum, Abe stated, "I would like Osaka G20 to be long remembered as the summit that started world-wide data governance. Let Osaka G20 set in train a new track for looking at data governance--call it the Osaka Track--under the roof of the WTO."[368] At the sidelines of the summit, Japan gathered G20 leaders and others participating in multilateral negotiations on e-commerce at the WTO to issue the Osaka Declaration on Digital Economy.[369] The Declaration was intended to fast-track efforts to settle international rules on the digital economy, including data flows, e-commerce, intellectual property, personal information, and cybersecurity. The signatories included all the G20 countries except for India, Indonesia and South Africa. Besides the G20, Singapore joined the declaration as an ardent supporter of rules to support cross-border data flows.

The Osaka Declaration included a separate initiative, *Data Free Flow with Trust*, which strongly bore the fingerprints of the EU's data governance approach. While the Osaka Declaration never gained meaningful traction, the *Data Free Flow with Trust* initiative continues under the auspices of the OECD, where the US, EU, and Japan continue active collaboration on government access to private sector data, among other topics.[370] As importantly, the EU engaged

[367] Koizumi, "Japan's pitch for free data flows 'with trust' faces uphill battle at G20 amid 'splinternet' fears."
[368] Shinzo Abe, "Speech by Prime Minister Abe at the World Economic Forum Annual Meeting: Toward a New Era of "Hope-Driven Economy"," (January 23, 2019). https://www.mofa.go.jp/ecm/ec/page4e_000973.html.
[369] LEADERS' SPECIAL EVENT (mofa.go.jp)
[370] Lauren Bernick and Koji Ouchi, "Panel Discussion: The OECD Effort on Developing Trusted Government Access to Private Sector Data," April 13, 2022, https://iapp.org/conference/past-conferences/GPS22/.

with Japan to coordinate efforts that would bring the United States closer to European regulatory preferences on data flows. Shortly after the launch of this initiative, the US-Japan Digital Free Trade Agreement ("DFTA") was signed on October 7, 2019. Although it does not mention DFFT, the DFTA attempts to strike a balance between "free flow" and "trust" in various fields, as noted by legal scholars Litt and Monroe-Sheridan.[371] Together, the EU and Japan could nudge the US toward better, more unified data regulation.

Even after Abe stepped down, Japan's leadership role in data governance continues today. The current Kishida administration plans to make realizing DFFT rules and norms a priority for Japan's G7 host year in 2023. Prime Minister Yoshihide Suga stood up a Digital Agency in 2021, partly as a response to the COVID pandemic.[372] "For decades, Japan was essentially a rule taker in the global economy, often assuming a defensive posture in international trade and rarely taking risks to champion new rules and norms. Abe changed all that, as his bold efforts on TPP, quality infrastructure, data governance underscore. At a time when the global economic order is under stress and the United States has pulled back from its traditional role as shaper of global economic rules, Abe's leadership was pivotal," concludes Matthew P. Goodman in his review of Abe's legacy after the former prime minister's assassination.[373] While Abe's leadership was the force that drove the EU and Japan to link strategic and economic partnerships with data governance, it was the EU's GDPR that shaped Abe's approach to data privacy and protection.

---

[371] David G. Litt and A. Reid Monroe-Sheridan, "The US-Japan Digital Trade Agreement and "Data Free Flow with Trust"," *US-Asia Law Institute*, February 3, 2022, https://usali.org/usali-perspectives-blog/the-us-japan-digital-trade-agreement-and-data-free-flow-with-trust.
[372] https://www.digital.go.jp/en/
[373] Matthew P. Goodman, "Shinzo Abe's Legacy as Champion of the Global Economic Order," *Commentary*, *Center for Strategic & International Studies*, 2022.

The remaining question is what the Japan case tells us about the Brussels Effect and the NIA. The evidence showed that neither theory completely captures the dynamic at play in the initial adequacy finding. However, the three agreements created institutions that serve vital purposes: 1) binding both parties to credible commitments to data flows with human rights; 2) creating cooperative institutions that share knowledge and insight about data flows, and; 3) creating institutions that could shift preferences about what is possible and desirable, shaping as much reflecting core national interests. The institutions thus created suggest that the NIA best describes the interactions between the two countries since the adequacy agreement was struck. The *DFFT* shows that this is precisely what happened. Through the DFFT, the EU and Japan both actively coordinate efforts to bring more countries into a sustainable global data flow arrangement and, in doing so, influence one another's attitudes and preferences. This dynamic is what the NIA would predict.

7 Lessons Learned and the Future of Data Governance

Global regulators increasingly frame data governance as a confrontation between democratic and authoritarian regimes. The great powers at the center of this confrontation were the subjects of this research. In summing up the negotiations between the EU and US in the most recent data transfer agreement, chief EU negotiator Bruno Gencarelli had this to say: "The Schrems II case is not really about the shortcomings of the US privacy protections alone. It is really about the rest of the world as well. The positive story is one of convergence on data flows: it is a distinguishing feature between like-minded countries and more authoritarian regimes."[374] On the one hand, advanced democracies are converging toward more European-style standards that facilitate the free flow of data across borders and protect the rights of its citizens. On the other hand, many illiberal countries are adopting aspects of European standards even as they reject the values those standards are intended to protect. All countries embrace the language of human rights as a conceptual *linga franca* for data privacy and protection in the United Nations and other intergovernmental forums, regardless of whether their legal systems in fact confer meaningful protections on individual citizens. This generates semantic confusion, making a global framework on data transfers a distant and challenging aspiration.

Conceptions of digital sovereignty and cyber-sovereignty, however inchoate, are increasingly influencing how private data is treated by governments. The impulse to shut off cross-border data flows under the banner of cyber-sovereignty is a growing trend not just among totalitarian regimes, but also among smaller democratic nations who feel vulnerable to the nations that control the infrastructure through which that data is transmitted and the

[374] Gencarelli and Hoff, interview.

facilities in which the data is stored. An unsolved but urgent question is how that data can flow across borders to encourage scientific and industrial innovation, and to ensure a competitive market economy. Again, the European Union has taken the lead with its suite of data governance regulations that are now being taken as a model for other countries as well. And again, we can expect that not all countries will adopt the European model in ways that respect the underlying human rights focus.

In the case study on China, we saw how government officials interpreted data governance not only as a tool to maintain domestic political control, but also as a means of defending it what it defines as its national sovereignty against the dangers of the international liberal order. A study of its comprehensive data governance legislation showed that the Brussels Effects explains the *de jure* adoption of European data privacy practices with little consideration for the human rights and dignitary component captured in the EU's *Charter of Fundamental Rights*. In China's case, the Brussels Effect is constrained to a very narrow understanding that might be better understood as a case of institutional isomorphism.

Japan, by contrast, pursued data governance as part of a strategic vision of itself as a more proactive international actor. While Japan did not formally adopt the language of human rights in its data privacy legislation or agreements with the EU, it has followed practices that in broadly harmonize with the EU conception. Moreover, since China's brutal takeover of Hong Kong and recent military exercises near Taiwanese airspace, Japanese citizens and government officials have increasingly come to promote democracy and human rights protections as an important narrative in their foreign policy.[375] The closer linkage of trade talks with data protection

[375] Green, *The Asia Chess Board*. At section 36:30.

talks encompasses a geopolitical framing aimed at balancing China's growing economic influence. China is rapidly developing an overwhelming data advantage over other countries in its Asian neighborhood due to the proliferation of its gargantuan data and internet-driven platforms that provide gaming, social media and consumer finance services. Since the establishment of mutual adequacy between Japan and the EU, the two sides have engaged in high levels of coordination to promote European standards. Given the success of the mutual adequacy model, it is conceivable that the European Commission will pursue it with other countries in the future.

Finally, the United States historically maintained a high degree of ideational rigidity in its understanding of data governance. Through a complex web of interactions across actors and jurisdictional boundaries, this attitude has gradually shifted. When the very first data transfer agreements were struck between the US and the EU, self-declared pro-market champions won a decisive victory. Over time, the narrative looked increasingly like the tortoise and the hare. The EU has played its role as tortoise well.

Given the philosophical disagreement among nations on baseline standards for global data governance, it seems unlikely that a global standard for data privacy protection will prevail. Shinzo Abe's vision of arriving at common rules for global data governance under the WTO umbrella is all but dead since the COVID pandemic. The disjuncture is not just philosophical but is also linked to the structural functioning of individual nations. A federal structure like the U.S. imposes limitations on legal change that an increasingly centralized entity like the EU struggles with to a lesser degree. Therefore, in the data governance space as in the trade area, one might expect to see more bilateral or regional mega-agreements among groups that are more closely

aligned philosophically and structurally. Countries with different legal systems will require exceptional policy entrepreneurship to effect closer convergence.

Nevertheless, the war in Ukraine has revived enthusiasm for the international liberal order. Francis Fukuyama contends that we may have Vladimir Putin to thank for saving the liberal world order.[376] There is truth to this from the perspective of data transfers. The very idea that the EU and US could overcome their long-standing philosophical clash over data flows in short order after the start of the war is testimony to the catalytic role the Ukraine invasion has played in catapulting issues previously relegated to second-order status to the top of the agenda for leaders on both sides of the Atlantic. The role of US companies in helping Ukraine resist Russian cyberattacks has brought into relief the heightened European need for cooperation with the US technology sector even as European Commission regulators seek to constrain it.[377] Similarly, the spread of disinformation and election-meddling has prompted the United States to draft better guardrails around the flow of information.

As Matthijs and Parsons recently noted, "if both sides recognize how much they can learn from each other's governance structures, the United States could end up being more prosperous by imitating certain EU-style rules, and the EU could rest on more stable political foundations by adopting some US-style institutional tools."[378] Add to this the Asian perspective, and we could see the emergence of a three-legged data governance structure based on

[376] Francis Fukuyama, "Francis Fukuyama: Putin's war on the liberal order," March 4, 2022, https://www.ft.com/content/d0331b51-5d0e-4132-9f97-c3f41c7d75b3.
[377] Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft on the Issues*, *Microsoft*, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
[378] Matthijs and Parsons, "Single-Market Power: How Europe Surpassed America in the Quest for Economic Integration."

multiple frameworks that forges new long-term stability. Neither political nor technological solutions alone will be sufficient.

8 Appendices

8.1 Appendix 1: Definitions

8.1.1 What is Data?

In the digital economy, nearly everything is based on data. Data are a series of zeros and ones that, when processed and assembled, represent ideas that are readable information. Where data is input, information is the output of processed data. The terminology is often applied inconsistently in the complex policy landscape of data flows. Thus, a popular term often used is personally identifiable information (PII). PII refers to data, such as names, birth date, place of birth, and other data from which one can determine a particular identity, rather than general information. The EU uses the terms data and information interchangeably. For example, the European Commission's website states: "Personal data is any information that relates to an *identified or identifiable living individual*. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data."[379]

In economic terms, data has no inherent value. However, in the 21st century, data processed into information assumes monumental importance. It has become a fifth factor of production along with land, labor, capital, and technology, and is recognized as such by the Chinese government, for one, in its official documents.[380] What makes data different from other factors of production is that data is "non-rival," meaning that it can be infinitely used, unlike natural

[379] "What is personal data?," accessed March 24, 2022, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.
[380] Liu, "The Rise of Data Politics: Digital China and the World."

resources, and “intangible,” which means that many people can use the same data simultaneously, or over time, without them being depleted. At the same time, access to data can be limited by technical or legal means, resulting in varying degrees of excludability.[381] Data localization requirements are one government policy lever used to limit data flows. This thesis, and indeed the GDPR, are focused on a particular type of data that is personally identifiable and can be exploited in violation of individual human rights. Other data types that are not the focus of this thesis largely include non-personal information or that which can be used to generate public goods. This refers, for example, to anonymized data used for fundamental medical research or artificial intelligence. It also includes economic data, such as GDP figures or trade flows, or sensitive government data, such as military secrets.

8.1.2 What is Data Privacy? What is Data Protection?

The term data protection is often used interchangeably with data privacy. This thesis follows the EU practice while noting that the EU formally distinguishes the two concepts. Data privacy is focused on the use and governance of personal data, for example, putting policies in place to ensure that consumers’ personal information is being collected, shared and used in appropriate ways. Security focuses predominantly on protecting data from malicious attacks and the exploitation of stolen data for profit. While security is necessary to protect data, it is not sufficient to address privacy. Because one theme of this thesis is the degree to which the EU can promote its European values through global GDPR adoption, the research is less concerned with important topics like data hacking or cybersecurity—however relevant these are—and

[381] Liu, "The Rise of Data Politics: Digital China and the World."

more concerned with the normative component of data privacy.[382] It relies on the tradition of defining privacy itself rather liberally as both the "freedom from" undue interference from outside actors, be they government, corporations, or other institutions, and as the individual "freedom to" control what others know about them as well as to define their narrative of themselves—limited, of course, by basic facts, and not simply magical thinking or what today is referred to as "alternative facts."[383]

Immanuel Kant, the most influential thinker in the continental European tradition, sets up a functional definition likely to have had the most influence on the GDPR's conception of privacy as a human right, namely as an inherent defense of personal dignity. Kant posits the individual as the "sovereign" agent of rational choice who is free precisely because s/he is able to make choices that at times override natural instinct.[384] For Kant, to be free is to make rational choices. In this way, we see the link between the principles of notification and consent as articulated in the GDPR and the protection of human rights and personal dignity. Exercising freedom, having the individual freedom of choice to determine what is known about us, is foundational to human dignity. Thus, a human rights approach in the data privacy context is often referred to as the "dignitary approach" because it is intended to broadly promote human dignity.

While there is a broad literature that more deeply evaluates the scope and nature of privacy, further discussion stretches beyond the purview of this thesis. In short, this thesis considers privacy as an instrument to achieve an end, which is protecting individual dignity. The larger

[382] "What Does Privacy Mean?," accessed November 22, 2021, https://iapp.org/about/what-is-privacy/.
[383] Jeroen et al van den Hoven, "Privacy and Information Technology," in *Stanford Encyclopedia of Philosophy* ed. Edward Zalta et al (Stanford, CA: Stanford University, 2020).
[384] Ari Ezra Waldman, *Privacy as Trust* (Cambridge: Cambridge University Press, 2018). Pgs. 14-15

problem of devising a taxonomy of privacy that is at once comprehensive and useful in generating principles or rules that can effectively be applied in courts of justice and by regulators is left to lawyers and philosophers.[385]

8.1.3 What are Human Rights?

We have just defined human rights as a defense of personal dignity. This is consistent with the definition of human rights put forth by the United Nations in its *Declaration of Human Rights*:

> *"Human rights are standards that recognize and protect the dignity of all human beings. Human rights govern how individual human beings live in society and with each other, as well as their relationship with the State and the obligations that the State have towards them.*
>
> *Human rights law obliges governments to do some things, and prevents them from doing others. Individuals also have responsibilities: in using their human rights, they must respect the rights of others. No government, group or individual person has the right to do anything that violates another's rights."*[386]

Beyond protecting individual privacy in a highly prescribed fashion, the EU takes the definition of human rights a step further in the digital economy context. The EU focuses on market competition by imposing on EU members states a requirement to level the playing field between the consumer (individual) and corporations. As Chapter II shows, the EU's approach to human rights explicitly targets monopolistic and anti-competitive market behaviors that harm consumers and proliferate what Farrell and Newman identify as "self-undermining feedback

[385] See, for example, extensive writings from Colin Bennett, including *The Privacy Advocates: Resisting the Spread of Surveillance*(2008); Daniel Solove, including *Understanding Privacy* (2012); and Ari Waldman, *Privacy as Trust* (2018).

[386] "What are Human Rights?," accessed December 12, 2022, https://www.unicef.org/child-rights-convention/what-are-human-rights.

effects."[387] These are mechanisms through which firms like Facebook or Google prosper at the expense of healthy democratic discourse in social media, for example, by profiting from the algorithmic promotion of divisive or false content. In other words, the EU sees the need to protect consumers and civil society from the more insidious effects of certain business models as part of its human rights mission. Protecting democracy, therefore, is partially a function of protecting the individual.

[387] Henry Farrell and Abraham Newman, "The Janus Face of the Liberal International Information Order: When Global Institutions are Self-Undermining," (2020).

8.2 Appendix 2: Case Study on the Impact of GDPR on Financial Services

While the GDPR was revolutionary for consumers, it also implied massive changes for financial services firms. From the firm perspective, the real revolution was in the business adaptations that the GDPR required *in concert with other regulations targeting finance subsectors*. It represented the concurrent response to both the GFC and the explosion of digitization in finance, which the EU rolled into its GFC response. These regulations included the Alternative Investment Fund Managers Directive (AIFMD) for the asset management sector in 2013,[388] the Anti-Money Laundering Directive (AMLD), the Second Payment Services Directive (PSD2), and MiFID II, among others. In the 2019 edition of its regulatory digest, the World Bank identified twenty-eight pieces of legislation, standards, guidelines, and supervisory documents that EU standard-setting bodies have issued on cybersecurity specifically for the financial sector. Twenty-five of the twenty-eight EU documents were introduced since the GDPR passed.[389] Collectively, these regulations imposed ever greater reporting obligations on financial intermediaries. Along with these new reporting requirements, in September 2020, the European Commission adopted a legislative proposal on digital resilience for the European financial sector, called DORA, as part of the EC's digital finance program. DORA aims to introduce a framework on digital operational resilience for European financial institutions, spelling out explicit requirements

[388] The AIFMD applies to alternative investments, many of which were largely unchecked prior to the 2008-09 GFC. The directive sets standards for marketing around raising private capital, risk monitoring and reporting, and overall accountability. The primary goal of the AIFMD is to protect investors as well as reduce systemic risk that alternative investment funds can pose.

[389] https://pubdocs.worldbank.org/en/361881595872293851/CybersecDigest-v5-Jul2020-FINAL.pdf

to address and mitigate ICT and cyber risks.[390] The combination of these regulations and the EU's Cybersecurity Directive of 2019 raised the stakes for financial services firms to the point that regulatory issues were elevated to the board of directors of major firms.[391]

An example of how GDPR worked in concert with other regulations is evident in the Second Payment Services Directive (PSD2), which introduced open banking to Europe. The GDPR took effect around the time that PSD2 was introduced. Open banking allows third-party financial service providers open access to consumer banking, transaction and other financial data from banks and non-bank financial institutions using application programming interfaces (APIs).[392] Open banking paved the way for a host of new digital banking products and services from non-traditional providers and has become a major source of innovation in the consumer banking industry. Fintech start-ups were the biggest beneficiaries of open banking, which was passed in response to the anti-competitive tendencies where the size of the data pool determines competitive strength. As pointed out by Arner et al., the success of open banking regulation is leading other jurisdictions, such as Australia, to consider similar regulations.[393] The dual push of GDPR and open banking enabled digital banking customers to not only protect their data, but also willingly share that data with third parties and fintech providers that offer

---

[390] Philipp S. Krüger and Jan-Philipp Brauchle, *The European Union, Cybersecurity, and the Financial Sector: A Primer*, Carnegie Endowment for International Peace (2021), https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055.

[391] Raising the discussion of data security to the board of directors' level of firms was an explicit recommendation of the World Bank report. See also the McKinsey report on the growing role of boards of directors in managing cybersecurity: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/boards-and-cybersecurity.

[392] https://www.investopedia.com/terms/o/open-banking.asp

[393] Douglas W. Arner et al., "The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II," *Stanford Journal of Law, Business & Finance* 25, no. 2 (Spring 2020).

innovative services. There are four important consequences of the willingness to share data. First, as more open banking products and services are launched and the benefits of data sharing become ever more apparent, the control and protection from the GDPR could help further drive consumer adoption of open banking services.

Second, as shown by a study from Aridor et al., although the opt-in requirement of GDPR resulted in a 12.5% drop in the intermediary-observed consumers, the consumers that did share data did so over longer periods, thereby increasing the value of the information they provided to advertisers.[394] The average value of consumers who continue to share data increases, which offsets some losses from consumer opt-outs. As for retail customers' awareness of their "right to be forgotten" under GDPR, a Deloitte survey of financial institutions showed that most banks are reporting a slight increase in data subject access requests (DSARs) since May 2018.[395] Consumer requests do not necessarily mean that individuals are asking to have their data deleted, only that they are asking to see the data that the bank holds on them.

Third, open banking together with GDPR address the thorny issue critics raised about GDPR raising the barriers to financial inclusion. By combining the privacy guarantees of the GDPR with the financial innovation of the fintechs, underserved communities are more likely to access the banking services they need.

Finally, together PSD2 and GDPR prompted retail banks and insurance firms to update their legacy technology systems. Retail banks and insurance companies typically keep personal

[394] Guy Aridor, Yeon-Koo Che, and Tobias Salz, "The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR," (NBER, 2020), Working Paper. https://www.nber.org/papers/w26900.

[395] Deloitte, *After the dust settles: How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on* (2019), https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf.

data for long periods in case it is needed in the future. The GDPR stipulates that businesses must not keep personal data for longer than needed, after which it should be erased or anonymized. To comply with GDPR's principles of data minimization, storage limits, and retention, banks have had to review their customer records policies. One of the key issues for retail banks and insurance was the fragmented collection of client data. A single customer's information might be housed in several databases, some unknown by key banking personnel. GDPR forced institutions to consolidate their consumer information, creating greater cost efficiencies. Consolidation also might yield insights into the customer base that were previously impossible because of data fragmentation.[396]

[396] PWC, *The EU General Data Protection Regulation (GDPR) in the banking industry* (2017), https://www.pwc.ch/en/publications/2017/gdpr_banking_industry_report_en.pdf; PWC, *The EU General Data Protection Regulation (GDPR) in the banking industry*.

8.3 Appendix 3: Understanding the Adequacy Process

Procedurally, countries reach out in confidence to the European Commission to discuss the possibility of an adequacy finding.[397] Third countries seeking adequacy status can decide for themselves whether they choose to announce that they are seeking adequacy status; most countries prefer not to risk the public disappointment of receiving an adverse finding by the EU. When making an assessment, EU authorities do not alone look at the applicant country's relevant legislation and case law. The GDPR requires that the Commission also consider a wide range of factors when assessing a country's personal data protections. These factors include:

- the rule of law, respect for human rights and freedoms, and the availability of effective administrative and judicial redress for individuals whose personal data is being transferred;
- the effectiveness of independent supervisory authorities with responsibility for enforcing the data protection rules; and
- the international commitments the country has entered into.

Adequacy decisions also consider a third country's relationship with and importance to the EU. For example, in the case of Argentina, the decision was granted in 2003 despite concerns about weaknesses in Argentine data protection laws.[398] Another example was in the EU's report on New Zealand, which discounted concerns about deficiencies in New Zealand's laws allowing for data that is routed through New Zealand to another country. The Commission

[397] Deputy Head of Unit Dr. Ralf Sauer, International Data Flows and Protection, DG Justice and Consumers, "What it means to have 'adequate' data protections in the eyes of the EU," interview by Nikhil Pahwa, *PrivacyNama 2021*, October 7, 2021, https://www.youtube.com/watch?v=YiQ1utjiBSo. Starting at 1:32/3:53.

[398] Cf. Commission Decision for EU's formal statement on Argentina. EU, 2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, (Brussels 2003).The country has since signed the Convention 108+ and upgraded its local laws to fall in line with new GDPR requirements. In granting Argentina Adequacy Status, the EU took into account the desire to establish a foothold in data governance leadership in Latin America. Argentina as the second largest economy in Latin America and a member of Mercosur was, therefore, an attractive target country.

decided that, given New Zealand's geographical distance from Europe, its size, and the nature of its economy, it was unlikely that those deficiencies would have much practical effect on EU data subjects.

In short, the Commission historically exercises considerable flexibility in extending adequacy status. This flexibility often involves changes in law or the adoption of practical "soft law"[399] or supplemental measures, as in the case of Japan. Such flexibility might also involve increasing protection for all personal data processed in the country or solely for personal data subject to the GDPR, i.e., that of EU citizens. Lastly, approval might limit the scope of adequacy status to particular territories or sectors, as in the case of Canada's finding, which applies only to the private sector. [400]

Adequacy is not open-ended, giving the EU continued leverage. Positive decisions require periodic review, at least every four years, to ensure that the country still offers an adequate level of protection. The European Parliament may request the Commission amend or withdraw an adequacy decision at any time.

The standards for adequacy have, at times, backfired on the EU. One prominent example is Australia, which sought adequacy status in 2001. The report of the EDPB identified eight areas in which Australian law did not offer adequate protection for personal data. The Australian Government declined to revise Australia's data protection laws to meet the required

[399] Soft law refers to rules that are neither strictly binding in nature nor completely lacking legal significance. In the context of international law, soft law refers to guidelines, policy declarations or codes of conduct which set standards of conduct. However, they are not directly enforceable.

[400] EU, 2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, (Brussels 2002).

standard and subsequently abandoned its bid for adequacy status. Nevertheless, more recently, Australia has updated its regulation of the digital economy, bringing it far closer in line with the GDPR.[401]

When introduced in 1995, one aim of adequacy status was to encourage other countries to adopt similar data protection laws to the EU. At first, adequacy requirements seemed to have had the desired effect, as Hong Kong, New Zealand, Japan, and many other nations upgraded their data protection regimes to facilitate trade flows. However, over time, businesses in countries that did not have adequacy opted to use the EC's alternative data transfer arrangements. In the absence of an adequacy finding, firms use Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) to engage in cross-border data flows.

SCCs are the most frequent alternative contractual arrangement through which firms conduct cross-border data transfers. SCCs set contractual terms and conditions which both the sender and the receiver of the personal data sign up to that ensure the rights and freedoms of the individual. SCCs safeguard data to a level required under the GDPR through contractual obligation in lieu of positive adequacy decisions. SCCs raise the cost of compliance for individual firms and thereby implicitly impose a trade barrier. Schrems II challenged SCCs in the ECJ, which ruled that they could not be used by firms like Facebook and similar companies who shared data with the US government.

[401] Graham Greenleaf, "'GDPR Creep' for Australian Businesses But Gap in Laws Widens," *UNSW Law Research Paper No. 18-54* (2018), https://ssrn.com/abstract=3226835.

BCRs are essentially corporate policies for data flows conducted internally by multinational companies that the Commission determines are adequate to protect personally identifiable data.[402] BCRs are applied in limited cases.

Finally, the GDPR allows for "derogations" to the cross-border personal data transfer restriction when a transfer may be made without an adequacy decision or appropriate safeguards. For example, a derogation is available where the data subject has given explicit informed consent to the transfer. Alternatively, derogations may apply when the transfer is necessary for an additional five reasons, which may include the execution of a contract between the data processor and the data subject. All these derogations must encompass what the EU calls a *legitimate interest*, which "are not overridden by the interests or rights and freedoms of the data subjects."[403]

Given the many derogations allowed, the question is why governments are incentivized to pursue adequacy in the first place. The EU argues that adequacy findings reduce market friction for companies doing business across borders and give a competitive advantage to those countries that obtain the adequacy finding. One example is the data processing company *Looq* based in a country that did not have an adequacy finding. In doing business, *Looq* would collect information from over 500 companies that held data on EU citizens. When the GDPR took effect, *Looq* was required to renegotiate all their 500 contracts to ensure compliance with the

[402] GDPR article 46.

[403] EU, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, (Brussels: Official Journal of the European Union, 2016). Article 49.

GDPR.[404] If Loog had been based in a country with adequacy, it would not need specific authorization to transfer data and, therefore, would not need SCCs.[405]

Generally, without an adequacy finding, large businesses will have a strong advantage over small businesses in complying, a common criticism leveled at the GDPR.[406] Through adequacy status, smaller companies are more likely to become competitors in the global marketplace, which is ultimately good for consumers. Adequacy status also facilitates the creation of a trusted business environment, which in turn will encourage consumers to share sensitive data more readily. It generates other positive externalities as well. As pointed out by European Commissioner for Justice, Consumers and Gender Equality Vera Jourova,

> *"For companies, compliance with the GDPR has proven to be an opportunity to put their data house in order by taking a closer look at what data they are collecting, what they use it for, how they keep and share it, and, whether they really need to collect and process all this data.*
> *Answering these questions has often allowed business to reduce exposure to unnecessary risks. But it also allows them to get a better idea of what data they hold and to develop a more trustworthy relationship with their customer and commercial partners.*
> *…companies … see other benefits from their privacy investments too, such as greater innovation, competitive advantages and lower costs relating to breaches."*[407]

SCCs and other arrangements are a target of criticism by privacy activists within Europe because they see them as a *de facto* loophole through which to circumvent the protection of

[404] Maarja Saluste, "Adequacy decisions: an opportunity for regulatory cooperation on data protection?," (2021). http://respect.eui.eu/wp-content/uploads/sites/6/2021/01/Saluste_Adequacy-decisions-Jan18-2021_RESPECT_final.pdf.
[405] Paul. Voigt, "The EU General Data Protection Regulation (GDPR) A Practical Guide," ed. Axel von dem Bussche (1st ed. 2017.). https://doi.org/10.1007/978-3-319-57959-7.
[406] Darcy et al Allen, "Some Economic Consequences of the GDPR," *Economics Bulletin, vol. 39, no. 2, pp. 785-797* (2019), https://doi.org/https://dx.doi.org/10.2139/ssrn.3160404.
[407] Vera Jourova, Speech by European Commission Věra Jourová at the 9th Annual European Data Protection and Privacy Conference: What next for European and global data privacy?, (European Commission, 2019).

human rights as defined by the European Charter. As nyob (an acronym for "none of your business"), the privacy activist group led by Max Schrems argued when the Privacy Shield was being challenged, "We don't have a problem with 'Standard Contractual Clauses', we have a problem with enforcement.[408] Indeed, enforcement is problematic since the EU cannot possibly have the institutional capacity to track and audit all the SCCs between companies. Some enforcement is done at the country level, but it is uneven. Ireland is the country most often cited as having weak enforcement.

[408] NOYB, *2019*, (Prep-Info: CJEU hears case on EU-US data transfers), https://noyb.eu/sites/default/files/2020-06/preppr_cjeu_en.pdf.

9 Bibliography

2020. "Apple Policy Statement: Our Commitment to Human Rights." https://s2.q4cdn.com/470004039/files/doc_downloads/gov_docs/2020/Apple-Human-Rights-Policy.pdf.

"2020 California Proposition 24 - Expand Consumer Privacy Election Results." *USA Today*. (November 3, 2020). Accessed December 21, 2021. https://www.usatoday.com/elections/results/race/2020-11-03-ballot_initiative-CA-8801/.

2021 Consumer Data Privacy Legislation. National Conference of State Legislatures (December 27, 2021). https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx.

2030 Digital Compass: The European Way for the Digital Decade. Brussels: European Commission, 2021.

Aaronson, Susan. "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security." *World Trade Review* 14, no. 4 (2015): 671-700.

Abe, Shinzo. "Speech by Prime Minister Abe at the World Economic Forum Annual Meeting: Toward a New Era of "Hope-Driven Economy"." January 23, 2019. https://www.mofa.go.jp/ecm/ec/page4e_000973.html.

Adams, Andrew A., Yohko Orito, and Kioshi Murata. "The Japanese Sense of Information Privacy." *AI & Society* (2009). https://doi.org/10.1007/s00146-009-0228-z.

"Adequacy Decisions: How the Eu Determines If a Non-Eu Country Has an Adequate Level of Data Protection." European Commission, accessed July 5, 2021, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Alaily, Rima, "Microsoft Supports New Rules for Gatekeepers," *EU Policy Blog*. *Microsoft* May 3, 2021, https://blogs.microsoft.com/eupolicy/2021/05/03/microsoft-supports-new-rules-for-gatekeepers/.

Alessi, Gil. "The Amazon Rainforest under Bolsonaro: A Story of Fire and Violence in Brazil." *El Pais USA*. English Edition. (September 16, 2021). https://english.elpais.com/usa/2021-09-16/the-amazon-rainforest-under-bolsonaro-a-story-of-fire-and-violence-in-brazil.html.

Anonymous. *Data Flows and Trade Agreements.* Open Rights Group (2021). https://www.openrightsgroup.org/publications/data-flows-and-trade-agreements/.

"Apple Privacy Policy." accessed June 4, 2022, https://www.apple.com/privacy/.

Arsenovic, Milica. "26+ Incredible Apple Statistics Showing Off Its Uniqueness ". (April 7, 2022). Accessed May 5, 2022. https://capitalcounselor.com/apple-statistics/.

Auslin, Michael. "Japan's New Realism." *Foreign Affairs* March/April 2016. https://www.foreignaffairs.com/articles/japan/2016-02-16/japans-new-realism.

"Austrian Dsb: Eu-Us Data Transfer to Google Analytics." noyb, Updated January 13, 2022, accessed August 1, 2022, https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal.

Bach, David, and Abraham L. Newman. "The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence." [In English]. Article. *Journal of European Public Policy* 14, no. 6 (09/01 / 2007): 827-46.

Bennett, Colin J. "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?". *Information Polity* 23 (2018): 239-46. https://doi.org/10.3233/IP-180002.

———. "The Privacy Advocates : Resisting the Spread of Surveillance." Cambridge, MA :: MIT Press, 2008. https://doi.org/10.7551/mitpress/7855.001.0001?locatt=mode:legacy.
Bernick, Lauren, and Koji Ouchi. "Panel Discussion: The Oecd Effort on Developing Trusted Government Access to Private Sector Data." April 13, 2022. https://iapp.org/conference/past-conferences/GPS22/.
Beuth, Patrick. "Das Soll Im Huawei-Gesetz Stehen." *Der Spiegel*. (December 12, 2020). Accessed March 3, 2021. https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-2-0-das-soll-im-huawei-gesetz-stehen-a-169932f8-94ab-42c2-903f-0fc84fb5fb93.
Bicchierai, Lorenzo-Franceschi, "Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document," *Motherboard*. *Vice*, April 26, 2022, https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
Bocchi, Marco, "Is the Eu Really More Precautionary Than the Us? Some Thoughts in Relation to Ttip Negotiations," *Blog of the European Journal of International Law*, August 9, 2016, https://www.ejiltalk.org/is-the-eu-really-more-precautionary-than-the-us-some-thoughts-in-relation-to-ttip-negotiations/.
Bradford, Anu. *The Brussels Effect.* Oxford: Oxford University Press, 2020.
———. " The Brussels Effect and China: Shaping Tech Standards: Insights from Anu Bradford." By Mercy Kuo. 01/07/2021, 2021. https://thediplomat.com/2021/01/the-brussels-effect-and-china-shaping-tech-standards/.
"How a Spanish Man Took on Google over Privacy Concerns and Won." Euronews Updated January 27, 2017, https://www.euronews.com/my-europe/2017/01/27/how-a-spanish-man-took-on-google-over-privacy-concerns-and-won.
Brill, Julie, "Microsoft's Commitment to Gdpr, Privacy and Putting Customers in Control of Their Own Data," *Microsoft on the Issues*, May 21, 2018, https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.
Burri, Mira. "The Regulation of Data Flows through Trade Agreements." *Georgetown Journal of International Law* 48 (08/28 2017): 407-48.
Büthe, Tim, and Walter Mattli. *The New Global Rulers: The Privatization of Regulation in the World Economy.* Princeton, NJ: Princeton University Press, 2011.
Calder, Kent E. "Japanese Foreign Economic Policy Formation: Explaining the Reactive State ". *World Politics* 40 (4) (1988): 517–41.
Carrapatoso, Astrid. "Climate Policy Diffusion: Interregional Dialogue in China–Eu Relations." *Global Change, Peace & Security* 23, no. 2 (2011/06/01 2011): 177-94. https://doi.org/10.1080/14781158.2011.580959. https://doi.org/10.1080/14781158.2011.580959.
"Ceos to Congress: Pass Comprehensive Nationwide Consumer Data Privacy Law ". Business Roundtable, September 10, 2019. https://s3.amazonaws.com/brt.org/BRT-CEOLetteronPrivacy-Finalv2.pdf.
Chakravorti, Bhaskar, Ajay Bhalla, and Ravi Shankar Chaturvedi. "Which Countries Are Leading the Data Economy?" *Harvard Business Review*. (January 24, 2019). https://hbr.org/2019/01/which-countries-are-leading-the-data-economy.
Chander, Anupam, and Uyen P. Le. "Data Nationalism ". *Emory Law Journal* 64, No. 3 (2015). https://ssrn.com/abstract=2577947
"China's Once-Shunned Entrepreneurs Join Communist Party." (October 6, 2007). https://www.spacedaily.com/reports/Chinas_once-shunned_entrepreneurs_join_Communist_Party_999.html.

China's Personal Information Protection Law: A Comparison of the First Draft, Second Draft, and the Final Document. (August 24, 2021). https://www.china-briefing.com/news/chinas-personal-information-protection-law-a-comparison-of-the-first-draft-the-second-draft-and-the-final-document/.

Chinapower. Podcast audio. The State of Japan-China Relations: A Conversation with Christopher Johnstone. https://chinapower.csis.org/podcasts/the-state-of-japan-china-relations/.

Cho, Eunsun. "The Social Credit System: Not Just Another Chinese Idiosyncracy." *Journal of Public and International Affairs* (2020). https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy.

Chorzempa, Martin, Paul Triolo, and Samm Sacks. *China's Social Credit System: A Mark of Progress or a Threat to Privacy?* (June 2018). https://www.piie.com/publications/policy-briefs/chinas-social-credit-system-mark-progress-or-threat-privacy.

Christakis, Theodore. *"European Digital Sovereignty".* Data Institute University Grenoble Alpes (December 2020).

Civil Code of the People's Republic of China. Beijing: People's Republic of China, 2020.

Cohen, Benjamin. *International Political Economy.* Princeton: Princeton University Press, 2008.

Commerce, U.S. Department of. "Statement from U.S. Secretary of Commerce Penny Pritzker on Eu-U.S. Privacy Shield." https://www.youtube.com/watch?v=XMal2UtceMI. Youtube: February 2, 2016.

"Consultative Committee." Council of Europe, accessed June 4, 2022, https://www.coe.int/en/web/data-protection/consultative-committee-tpd.

"The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the Eu-Us Data Protection Shield." news release., 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

Creemers, Rogier. "China's Emerging Data Protection Framework." (2021). https://doi.org/http://dx.doi.org/10.2139/ssrn.3964684.

———. "Party Ideology and Chinese Law." In *Law and the Party in China: Ideology and Organisation*. Cambridge: Cambridge University Press, 2021.

———. "The Pivot in Chinese Cybergovernance: Integrating Internet Control in Xi Jinpingæs China." [In English]. Article. *China Perspectives*, no. 4 (01/01 / 2015): 5-14.

Creemers, Rogier, Graham Webster, and Paul Triolo. *Cybersecurity Law of the People's Republic of China (Translation)*. Stanford: Stanford University Digichina, 2018.

"Cross-Border Privacy Rules certification." BBB National Programs, accessed July 1, 2022, https://bbbprograms.org/programs/all-programs/GlobalPrivacyDivision/CrossBorderPrivacyRules.

Cunningham, Edward, Tony Saich, and Jesse Turiel. *Understanding Ccp Resilience: Surveying Chinese Public Opinion through Time.* Harvard Kennedy School Ash Center (2020).

Dang, Sheila, and Nivedita Balu. "Facebook Ad Revenue Seen Feeling Brunt of Apple Privacy Changes." October 25, 2021. https://www.reuters.com/technology/facebook-ad-revenue-seen-feeling-brunt-apple-privacy-changes-2021-10-25/.

"Data Protection." European Data Protection Supervisor, accessed September 24, 2021, https://edps.europa.eu/data-protection/data-protection_en.

Data Protection Laws of the World. 2021.

Declaration for the Future of the Internet. U.S. Department of State, 2022.

DeNardis, Laura, and Michael Murphree. "Digital Standards." *Digital Economy & Security Collaborative*. Georgetown University Mortara Center. February 17, 2022.

Detsch, Jack. "Abe's Legacy Will Outlive Him." (July 8, 2022). https://foreignpolicy.com/2022/07/08/shinzo-abe-assassination-japan-indo-pacific-security/.

"Development as a Human Right : Legal, Political, and Economic Dimensions." edited by Bård-Anders Andreassen and Stephen P. Marks. Boston: Harvard School of Public Health, François-Xavier Bagnoud Center for Health and Human Rights, 2006.
Dickson, Bruce. *The Party and the People: Chinese Politics in the 21st Century.* Princeton: Princeton University Press, 2021.
Diggelmann, Oliver, and Maria Nicole Cleis. "How the Right to Privacy Became a Human Right." *Human Rights Law Review* 14, no. 3 (2014): 441-58. https://doi.org/10.1093/hrlr/ngu014. https://doi.org/10.1093/hrlr/ngu014.
Ding, Jason. *China Internet Report.* (March 26, 2021). https://www.bain.com/insights/china-internet-report/.
Ding, Jeffrey. *Stanford University Hai Seminar Series: The Rise and Fall of Great Technologies and Powers*. HAI Stanford University.
Disis, Jill. "China Fines Alibaba, Tencent and Baidu for More Antitrust Violations." (November 22, 2021). Accessed March 10, 2022. https://www.cnn.com/2021/11/22/tech/alibaba-tencent-fines-intl-hnk/index.html.
Docksey, Christopher, "Schrems Ii and Individual Redress—Where There's a Will, There's a Way," *Lawfare*, October 12, 2020, https://www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way.
Doneda, Danilo. "Expert Interview on Brazil Data Protection Law." By Nicola Daniel. February 22, 2022.
Drezner, Daniel W. "All Politics Is Global : Explaining International Regulatory Regimes." Princeton, N.J.: Princeton University Press, 2007. http://www.loc.gov/catdir/toc/ecip0615/2006017741.html.
EC. *Commission Implementing Decision (Eu) 2019/419*. Brussels: European Commission, 2019.
"What Is Personal Data?", accessed March 24, 2022, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.
Economy, Elizabeth. *The Third Revolution.* Oxford: Oxford University Press, 2018.
———. *The World According to China.* Wiley Publishers, 2021.
Envall, H.D.P. "The 'Abe Doctrine': Japan's New Regional Realism." *International Relations of the Asia-Pacific* 20, (2020) 31–59 (2018). https://doi.org/10.1093/irap/lcy014.
Erie, Matthew Steven, and Thomas Streinz. "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance." *54 N.Y.U. J. Int'l L. & Pol. 1* (2021). https://ssrn.com/abstract=3810256
"Eu-China: Commission and China Hold First High-Level Digital Dialogue." news release., September 10, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1600.
EU. *2002/2/Ec: Commission Decision of 20 December 2001 Pursuant to Directive 95/46/Ec of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act*. Brussels, 2002.
———. *2003/490/Ec: Commission Decision of 30 June 2003 Pursuant to Directive 95/46/Ec of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina*. Brussels, 2003.
———. *Commission Implementing Decision (Eu) 2019/419 of 23 January 2019 Pursuant to Regulation (Eu) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan under the Act on the Protection of Personal Information* Brussels, 2019.
"Eu Data Protection Directive." Electronic Privacy Information Center (EPIC), accessed October 1, 2021, https://archive.epic.org/privacy/intl/eu_data_protection_directive.html.
"Eu to Ban Data Localisation Restrictions as Ambassadors Approve Deal on Free Flow of Data." news release., June 20, 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/eu-to-ban-data-localisation-restrictions-as-ambassadors-approve-deal-on-free-flow-of-data/.

"The Eu Wants to Set the Rules for the World of Technology." *The Economist*, February 20, 2020.
"European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework." news release., March 25, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.
A European Strategy for Data. European Commission, 2020.
European Union. "Charter of Fundamental Rights of the European Union." 2012.
Exchanging and Protecting Personal Data in a Globalised World. Brussels: European Commission 2017.
"Fact Sheet on China's Foreign Ngo Law." The China NGO Project, Updated November 1, 2017, accessed March 10, 2022, https://www.chinafile.com/ngo/latest/fact-sheet-chinas-foreign-ngo-law.
Fahey, Elaine. *The Eu as Global Digital Actor.* Modern Studies in European Law. Oxford: Hart Publishing, 2022.
Fairfield, J., and C. Engel. "Privacy as a Public Good." In *Privacy and Power: A Transatlantic Dialogue in the Shadow of the Nsa-Affair* edited by R. Miller (Ed.), 95-128. Cambridge: Cambridge University Press, 2017.
Farrell, Henry, and Abraham Newman. "The New Interdependence Approach: Theoretical Development and Empirical Demonstration." *Review of International Political Economy* 23, no. 5 (2016/09/02 2016): 713-36. https://doi.org/10.1080/09692290.2016.1247009.
———. *Of Privacy and Power.* Princeton and Oxford: Princeton University Press, 2019.
Farrell, Henry, and Bruce Schneier. "Common Knowledge Attacks on Democracy." *Research Publication No. 2018-7*. (2018).
Frankenreiter, Jens. "The Missing 'California Effect' in Data Privacy Laws." *Yale Journal on Regulation, forthcoming* (2021). https://doi.org/http://dx.doi.org/10.2139/ssrn.3883728.
Fu, Diana. *Mobilizing without the Masses: Control and Contention in China.* Cambridge Studies in Contentious Politics. Cambridge: Cambridge University Press, 2017. doi:DOI: 10.1017/9781108354707. https://www.cambridge.org/core/books/mobilizing-without-the-masses/FE8DA14FD770D0FACF35E9979A3BB8DA.
Fu, Tao. "China's Personal Information Protection in a Data-Driven Economy: A Privacy Policy Study of Alibaba, Baidu and Tencent." *Global Media and Communication* 15, no. 2 (2019): 195-213. https://doi.org/10.1177/1742766519846644. https://journals.sagepub.com/doi/abs/10.1177/1742766519846644.
———. "China's Personal Information Protection in a Data-Driven Economy: A Privacy Policy Study of Alibaba, Baidu and Tencent." *Global Media and Communication* 15 (05/27 2019): 174276651984664. https://doi.org/10.1177/1742766519846644.
Fukuyama, Francis. "Francis Fukuyama: Putin's War on the Liberal Order." March 4, 2022. https://www.ft.com/content/d0331b51-5d0e-4132-9f97-c3f41c7d75b3.
———. "The Origins of Political Order." New York: Farrar, Strauss, Giroux, 2011. https://ebookcentral.proquest.com/lib/jhu/detail.action?docID=689270.
———. *Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy.* New York: Farrar, Straus and Giroux, 2014.
Garrick, John, and Yan Chang Bennett. ""Xi Jinping Thought": Realisation of the Chinese Dream of National Rejuvenation?". Article. *China Perspectives*, no. 1/2 (2018): 99-105.
Gencarelli, Bruno. "In Conversation with Mr. Gencarelli, the Eu's Head of International Transfers." By Lore Leitner. *IAPP Europe Data Protection Congress*. IAPP. November 17, 2021.
Gencarelli, Bruno, and Christopher Hoff. "Eu-U.S. Privacy Shield and Teh Future of Trans-Atlantic Data Flows." By Brian Scarpelli. *IAPP Global Privacy Summit 2022*. https://iapp.org/conference/past-conferences/GPS22/.
The Geopolitics of Semiconductors The Eurasia Group (September 2020).

Geradin, Damien, Dimitrios Katsifis, and Theano Karanikioti. "Google as a De Facto Privacy Regulator: Analysing the Privacy Sandbox from an Antitrust Perspective." Article. *European Competition Journal* 17, no. 3 (2021): 617-81. https://doi.org/10.1080/17441056.2021.1930450.

Gesetz Zur Erhöhung Der It-Sicherheit Mit Koali-Tions-Mehrheit Beschlossen. Deutscher Bundestag (German national parliament), 2021.

Gilson, Julie. *Eu-Japan Relations and the Crisis of Multilateralism.* London and New York: Routledge, 2020. https://www.taylorfrancis.com/books/9780429326134.

"Global Europe: Competing in the World." In *European Encyclopedia of Law*. https://europeanlaw.lawlegal.eu/global-europe-competing-in-the-world/.

GOJ, and Government of Japan. *National Security Strategy*, 2013.

Goldsmith, Jack, and Stuart Russell. "Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations." *Aegis Series Paper No. 1806*. (2018).

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet?* : Oxford University Press, 2006.

Goodman, Matthew P., "Shinzo Abe's Legacy as Champion of the Global Economic Order," *Commentary*. *Center for Strategic & International Studies*, 2022.

"Google Privacy Policy Us." accessed September 24, 2022, https://policies.google.com/privacy?hl=en-US#infochoices.

Green, Michael. *The Asia Chess Board.* Podcast audio. The Asia Shogi-board: Strategic Insights with Yoichi Funabashi, 2021.

———. *The Asia Chess Board.* Podcast audio. The Legacy of Shinzo Abe, 2022.

———, "Shinzo Abe's Decision to Step Down," *Critical Questions*. *Center for Strategic and International Studies*, 2020, https://www.csis.org/analysis/shinzo-abes-decision-step-down.

Greene, Jamal. *How Rights Went Wrong* New York: Houghton Mifflin, 2021.

Greenleaf, Graham. *Asian Data Privacy Laws, Trade and Human Rights Perspective.* Oxford: Oxford University Press, 2014.

———. "'Gdpr Creep' for Australian Businesses but Gap in Laws Widens." *UNSW Law Research Paper No. 18-54* (2018). https://ssrn.com/abstract=3226835.

———. Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (Gdpr) in Brussels & New Delhi. 2018.

———. "Global Data Privacy Laws 2021: Despite Covid Delays, 145 Laws Show Gdpr Dominance," *169 Privacy Laws & Business International Report, UNSW Law Research Paper No. 21-60*(2021). https://doi.org/http://dx.doi.org/10.2139/ssrn.3836348

Gribakov, Andrei, "Road to Adequacy: Can California Apply under the Gdpr?," *Lawfareblog.com*, 2019, https://www.lawfareblog.com/road-adequacy-can-california-apply-under-gdpr.

Griffiths, James. *Great Firewall of China.* Bloomsbury Publishing, 2019.

"Guidelines of the Anti-Monopoly Commission of the State Council for Anti-Monopoly in the Platform Economy (国务院反垄断委员会关于平台经济领域的反垄断指南（2021 年 2 月 7 日国务院反垄断委员会印发）)." Government of the People's Republic of China accessed March 10, 2021, https://gkml.samr.gov.cn/nsjg/fldj/202102/t20210207_325967.html.

Gunst, Simon, and Ferdi De Ville. "The Brussels Effect: How the Gdpr Conquered Silicon Valley." *European Foreign Affairs Review* 26, No. 3 (2021).

Guyunn, Jessica. "Amazon, at&T, Google Push Congress to Pass Online Privacy Bill to Preempt Stronger California Law." *USA Today*. (September 26, 018). https://www.usatoday.com/story/tech/news/2018/09/26/amazon-att-google-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002/.

Haas, Ernst B. . *The Uniting of Europe.* Stanford: Stanford Univ. Press, 1958.

Hao, Karen. "Inside China's Unexpected Quest to Protect Data Privacy." *MIT Technology Review*. (August 19, 2020 2020). https://www.technologyreview.com/2020/08/19/1006441/china-data-privacy-hong-yanqing-gdpr/.
Harari, Yuval. "Why Technology Favors Tyranny." *The Atlantic*, no. October 2018.
Hatmaker, Taylor. "Congress Probes Period Tracking Apps and Data Brokers over Abortion Privacy Concerns." TechCrunch, July 8, 2022. https://techcrunch.com/2022/07/08/house-oversight-letter-abortion-period-apps-data-brokers/.
Heilmann, S., and E. Perry. "Embracing Uncertainty: Guerilla Policy Style and Adaptive Governance in China." In *Mao's Invisible Hand: The Political Foundation of Adaptive Governance in China*, edited by S. Heilman and E. Perry, 1-29. Cambridge, MA: Harvard University Press, 2011.
Helleiner, Eric, and Stefano Pagliari. " Between the Storms: Patterns in Global Financial Governance, 2001-2007." In *Global Financial Integration Thirty Years On: From Reform to Crisis*, edited by Jasper Blom Geoffrey R.D. Underhill, and Daniel Mügge, eds., 42-57. Cambridge: Cambridge University Press, 2010.
Hern, Alex. "Facebook Moves 1.5bn Users out of Reach of New European Privacy Law." *The Guardian*. (April 19, 2018). Accessed November 24, 2021. https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law.
Hille, Kathrin. "Tsmc: How a Taiwanese Chipmaker Became a Linchpin of the Global Economy." *Financial Times*, March 24, 2021.
Horwitz, Jeff. "The Facebook Files." *Wall Street Journal* (New York), October 1, 2021. https://www.wsj.com/articles/the-facebook-files-11631713039.
Huang, Yehan, and Mingli Shi. "Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law." (June 8, 2021). https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/.
Hurel, L. M., and L.C. Lovato. ""Cyber-Norms Entrepreneurship? Understanding Microsoft's Advocacy on Cybersecurity"." In *Governing Cyberspace: Behaviour, Power, and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield, 2020.
"Ccpa-/Cpra-Related Legislation Tracker." Updated October 10, 2022, accessed October 1, 2022, https://iapp.org/resources/article/ccpa-cpra-related-legislation-tracker/.
IAPP. "Eu's Strategy for Data: What the Dsa, Dma, Dga Mean for Privacy." December 12, 2021 2021.
"What Does Privacy Mean?", accessed November 22, 2021, https://iapp.org/about/what-is-privacy/.
Igo, Sarah. *The Known Citizen.* Boston: Harvard University Press, 2018.
"Us, Uk and Eu Impose Significant Sanctions and Export Controls in Response to Russia's Invasion of Ukraine." Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, Updated February 26, 2022, accessed June 4, 2022, https://www.skadden.com/insights/publications/2022/02/us-uk-and-eu-impose-significant-sanctions.
Jervis, Robert. "Realism, Neoliberalism, and [International] Cooperation: Understanding the Debate." [In English]. Article. *International Security* 24, no. 1 (06/01 / 1999): 42-63.
Jiang, Zemin. *Report at 16th Party Congress on Nov 8, 2002*. Beijing: Ministry of Foreign Affairs of the Republic of China, 2002.
"Jack Ma: Traditional Banks Are Operating with a 'Pawn Shop' Mentality." accessed 05/09/2022, https://www.thinkchina.sg/jack-ma-traditional-banks-are-operating-pawn-shop-mentality.
"Judgement of the Court." edited by Court of Justice of the European Union, 2015. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362.

Keane, Jonathan. "From California to Brazil, Europe's Privacy Laws Have Created a Recipe for the World." (April 8, 2021). Accessed January 15, 2022. https://www.cnbc.com/2021/04/08/from-california-to-brazil-gdpr-has-created-recipe-for-the-world.html.
Koizumi, Masumi. "Japan's Pitch for Free Data Flows 'with Trust' Faces Uphill Battle at G20 Amid 'Splinternet' Fears." *Japan Times*. (June 27, 2019).
Kostka, Genia. "China's Social Credit Systems Are Highly Popular – for Now." (September 17, 2018). https://merics.org/en/analysis/chinas-social-credit-systems-are-highly-popular-now.
KPMG, and China. *Overview of China's Cybersecurity Law.* (2017). https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.
Kratochvil, Petr. "The End of Democracy in the Eu? The Eurozone Crisis and the Eu's Democratic Deficit." *Journal of European Integration* Vol. 41 Issue 2 (2019).
Krempl, Stefan. "It-Sicherheitsgesetz 2.0: "Mittelfinger Ins Gesicht Der Zivilgesellschaft" ". (December 10, 2020). Accessed March 3, 2021. https://www.heise.de/news/IT-Sicherheitsgesetz-2-0-Mittelfinger-ins-Gesicht-der-Zivilgesellschaft-4986032.html.
KRISTOF, NICHOLAS D. . "Beijing Journal: Where Each Worker Is Yoked to a Personal File." *The New York Times* (New York), March 16, 1992.
Kuner, Christopher. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law." (02/06 2012).
———. "An International Legal Framework for Data Protection: Issues and Prospects." *Computer Law & Security Review* 25, no. 4 (July 2009 2009): 307-17.
Lange, Bernd. "Eu-Mercosur: The Bolsonaro Factor." *IPS*. (May 3, 2019). https://www.ips-journal.eu/topics/foreign-and-security-policy/eu-mercosur-the-bolsonaro-factor-3296/.
Lapowsky, Issie. "Inside the Closed-Door Campaigns to Rewrite California Privacy Law, Again: How Google, Facebook, the Eff and Others Lobbied Alastair Mactaggart — and What They Managed to Get." *Protocol*. (February 6, 2020). Accessed Nov. 24, 2021. https://www.protocol.com/inside-california-privacy-law-redo.
"Leading Import Countries for Motor Vehicles from Germany in 2021, by Value of Exports." Statista, accessed September 26, 2021, https://www.statista.com/statistics/587701/leading-import-countries-german-motor-vehicles-by-export-value/.
Lee, Bertram. "Federal Privacy Legislation That Protects Civil Rights Is Critical for All Americans." *The Hill*. (July 21, 2022). Accessed July 25, 2022. https://thehill.com/opinion/congress-blog/3568525-federal-privacy-legislation-that-protects-civil-rights-is-critical-for-all-americans/.
Lee Rainie, and et al. *Americans and Privacy: Confused, Concerned, and Feeling Lack of Control over Their Personal Information.* (2019). https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
Lieberthal, Kenneth. "Introduction: The 'Fragmented Authoritarianism' Model and Its Limitations." In *Bureaucracy, Politics, and Decision Making in Post-Mao China*, edited by Kenneth Lieberthal and David M. Lampton. Berkeley :: University of California Press, 1992.
Lieberthal, Kenneth G. ""Introduction: The 'Fragmented Authoritarianism' Model and Its Limitations,"." In *Bureaucracy, Politics, and Decision-Making in Post-Mao China*, edited by Lieberthal and David M. Lampton (eds.). Berkeley: University of California Press, 1992.
Litt, David G., and A. Reid Monroe-Sheridan, "The Us-Japan Digital Trade Agreement and "Data Free Flow with Trust"." *US-Asia Law Institute*, February 3, 2022, https://usali.org/usali-perspectives-blog/the-us-japan-digital-trade-agreement-and-data-free-flow-with-trust.
Liu, Lizhi. "The Rise of Data Politics: Digital China and the World." *Studies in Comparative International Development* 56, no. 1 (2021/03/01 2021): 45-67. https://doi.org/10.1007/s12116-021-09319-8.

Liu, Xiao. "Understanding China's Governance Space around Personal Data." In *Essays on the Rise of China and Its Implications*, edited by Abraham M. Denmark and Lucas Myers. Washington, D.C.: Wilson Center, 2021.
Lord, Nate, "What Is the Data Protection Directive," *Digital Guardian's Blog*, September 12, 2018, https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.
Lu, Xing. "The Rhetoric of Mao Zedong Transforming China and Its People." University of South Carolina Press, 2017. https://muse.jhu.edu/book/51909/.
Luis Alberto Montezuma, FIP. "Obtaining Adequacy Standing for Colombia." (August 2, 2018). https://iapp.org/news/a/obtaining-adequacy-standing-for-colombia/.
Ma, Winston. "China Is Waking up to Data Protection and Privacy. Here's Why That Matters." (11/12/2019). https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline/.
MACASKILL, EWEN, and GABRIEL DANCE. "Nsa Files: Decoded." *The Guardian*, November 1, 2013. https://www.theguardian.com/us-news/the-nsa-files.
Madiega, Tambiama. "Digital Sovereignty for Europe." *EPRS Ideas Paper* (July 2020). https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.
Majone, Giandomenico. "The Rise of the Regulatory State in Europe." In *West European Politics*, edited by Wolfgang C. Muller and Vincent Wright, 77-101, 1994.
Manger, Mark. "Competition and Bilateralism in Trade Policy: The Case of Japan's Free Trade Agreements." *Review of International Political Economy* 12, no. 5 (2005): 804-28. https://doi.org/http://www.tandfonline.com/loi/rrip20.
Manyika, James, and et al. *Digital Globalization: The New Era of Global Flows.* (2016).
Matthijs, Matthias, and Craig Parsons. Muscles in Brussels: The European Union's Economic Authority in Comparative and Theoretical Perspective. 2019.
———. "Single-Market Power: How Europe Surpassed America in the Quest for Economic Integration." *Foreign Affairs* May/June 2022.
———. Why Did Europe's Single Market Surpass America's? April 27, 2021.
McNamara, Kathleen. "European Foreign Policy." Chap. 7 In *The Politics of Everyday Europe*, 135-60. Oxford: Oxford University Press, 2015.
McNamara, Kathleen R. "Authority under Construction: The European Union in Comparative Political Perspective." *JCMS: Journal of Common Market Studies* 56, no. 7 (2018): 1510-25. https://doi.org/https://doi.org/10.1111/jcms.12784. https://onlinelibrary.wiley.com/doi/abs/10.1111/jcms.12784.
Mellor, Sophie. "Apple and Google Criticize the New Eu Digital Markets Act That Will Radically Change the Way They Have Operated for the Past 20 Years." *Fortune*, March 25, 2022. https://fortune.com/2022/03/25/apple-google-criticize-eu-digital-markets-act/.
Mertha, Andrew. ""Fragmented Authoritarianism 2.0": Political Pluralization in the Chinese Policy Process." *The China Quarterly* Dec 2009, No. 200 (2009): 995-1012. https://www.jstor.org/stable/27756540.
Mertha, Andrew C. "China's "Soft" Centralization: Shifting Tiao/Kuai Authority Relations." [In English]. Article. *China Quarterly* 184 (12/01 / 2005): 791-810.
"Microsoft by the Numbers." accessed August 25, 2022, https://news.microsoft.com/bythenumbers/en/homepage.
"Microsoft Global Human Rights Statement." https://www.microsoft.com/en-us/corporate-responsibility/human-rights-statement?activetab=pivot_1%3aprimaryr5.
Miller, Alice. "Only Socialism Can Save China; Only Xi Jinping Can Save Socialism." Article. *China Leadership Monitor* 56 (Spring2018 2018): 1-9.

Morton, Katherine. "China's Global Governance Interactions." In *China and the World*, edited by David Shambaugh. Oxford: Oxford University Press, 2020.
Murgia, Madhumita. "Inside China's Controversial Mission to Reinvent the Internet." *Financial Times* (London), March 27, 2020.
National Tracking Poll #2206078 Crosstabulation Results. Morning Consult + Politico (June 10-12, 2022). https://assets.morningconsult.com/wp-uploads/2022/06/14130054/2206078_crosstabs_POLITICO_RVs_v1_06-15-22_SH.pdf.
Naughton, Barry. "China's Response to the Global Crisis, and the Lessons Learned." In *The Global Recession and China's Political Economy*, edited by Dali L. Yang: Palgrave Macmillan, 2012.
Newman, Abraham. *Protectors of Privacy.* Ithaca: Cornell University Press, 2008.
Newman, Abraham, and David Bach. "The European Union as Hardening Agent: Soft Law and the Diffusion of Global Financial Regulation." [In English]. Article. *Journal of European Public Policy* 21, no. 3 (01/01 / 2014): 430-52.
Ng, Alfred. "Tech Giants Ask Congress for a Data Privacy Bill to Bypass State Laws." *CNET*. (September 10, 2019).
Nguyen, David, and Marta Paczos. "Measuring the Economic Value of Data and Cross-Border Data Flows." (2020). https://doi.org/doi:https://doi.org/10.1787/6345995e-en. https://www.oecd-ilibrary.org/content/paper/6345995e-en.
Nocetti, Julien. " Is Europe a "Digital Colony" of the United States?". *Politique étrangère* vol. , no. 3, , pp. (2021): 51-63. https://doi.org/ https://doi.org/10.3917/pe.213.0051
"Nsa Prism Program Taps in to User Data of Apple, Google and Others." (2013). https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
Nye, Joseph S., and Robert O. Keohane. "Transnational Relations and World Politics: An Introduction." *International Organization* 25, no. 3 (1971): 329-49. https://doi.org/10.1017/S0020818300026187.
Oatley, Thomas. "The Reductionist Gamble: Open Economy Politics in the Global Economy." *International Organization* 65 (2011): 311 - 41.
———. "Toward a Political Economy of Complex Interdependence." *European Journal of International Relations* 25, no. 4 (2019): 957-78.
OECD. *Oecd Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD, 1980.
Pearson, Margaret. "Variety within and Without: The Political Economy of Chinese Regulation." In *Beyond the Middle Kingdom Comparative Perspectives on China's Capitalist Transformation*, edited by Scott Kennedy. Palo Alto: Stanford University Press, 2011.
Piper, DLA. *Gdpr Fines and Data Breach Survey: January 2022.* (2022).
Posner, Elliot. "Making Rule for Global Finance: Transatlantic Regulatory Cooperation at the Turn of the Millennium." *International Organization* 63:4 (October) (2009): 665-99.
PPC. *Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission*, 2018.
"The Precautionary Principle." In *European Encyclopedia of Law: European Union Regulations*. https://europeanlaw.lawlegal.eu/the-precautionary-principle/.
Presidential Policy Directive -- Signals Intelligence Activities. The White House, 2014.
Putnam, Robert D. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42, no. 3 (1988): 427-60. http://www.jstor.org/stable/2706785.
Rash, Wayne. "Eu, U.S. Privacy Shield Deal Greeted with Claims It's Meaningless." Article. *eWeek* (2016): 2-2.

The Right to Development: China's Philosophy, Practices and Contributions. Beijing: People's Republic of China, 2016.
Rithmire, Meg, and Hao Chen. "The Emergence of Mafia-Like Business Systems in China." *The China Quarterly* 248, no. 1 (2021): 1037-58. https://doi.org/10.1017/S0305741021000576.
Rossi, Agustín. "How the Snowden Revelations Saved the Eu General Data Protection Regulation." *The International Spectator* 53, no. 4 (2018/10/02 2018): 95-111. https://doi.org/10.1080/03932729.2018.1532705. https://doi.org/10.1080/03932729.2018.1532705.
"Analysis of China's Draft Personal Information Protection Law." Arnold & Porter, 2020, https://www.arnoldporter.com/en/perspectives/publications/2020/11/analysis-of-chinas-draft-pip-law.
Saluste, Maarja. *Adequacy Decisions: An Opportunity for Regulatory Cooperation on Data Protection?* (2021).
Sauter, Wolf. "Proportionality in Eu Law: A Balancing Act?". *Cambridge Yearbook of European Legal Studies* 15 (2013): 439-66. https://doi.org/10.5235/152888713809813611.
Schneier, Bruce. *The Coming Ai Hackers.* Belfer Center, Harvard University (2021). https://www.belfercenter.org/publication/coming-ai-hackers.
Schwartz, Paul M. "Global Data Privacy: The Eu Way." [In English]. *New York University Law Review* 94, no. 4 (2019): 771.
———. "Preemption and Privacy ". *Yale Law Journal* UC Berkeley Public Law Research Paper No. 1404082 (2009). https://ssrn.com/abstract=1404082
Segal, Adam. "When China Rules the Web." *Foreign Affairs*, no. Sept/Oct 2018 (2018). https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.
Shead, Sam L. "Amazon Hit with $887 Million Fine by European Privacy Watchdog." (July 30, 2021). https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html.
Shih, Willy. "Is It Time to Rethink Globalized Supply Chains?". *MIT Sloan Management Review* 61, 4, no. Summer 2020: 1-3.
Simon, Lius. "Europe, the Rise of Asia and the Future of the Transatlantic Relationship." *International Affairs* 91, no. 5 (September 2015 2015): 969-89. https://doi.org/https://doi.org/10.1111/1468-2346.12393.
Smith, Brad, "Answering Europe's Call: Storing and Processing Eu Data in the Eu," *Micosoft EU Policy Blog*, May 6, 2021, https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/.
———, "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft on the Issues*. *Microsoft*, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
Solis, Mireya, and Shujiro Urata. "Abenomics and Japan's Trade Policy in a New Era." *Asian Economic Policy Review* 13 (2018): 106-23.
Solove, Daniel, "A Faustian Bargain: Is Preemption Too High a Price for a Federal Privacy Law?," Daniel Solove ed. *Privacy & Security Blog*, July 22, 2022, https://teachprivacy.com/a-faustian-bargain-is-preemption-too-high-a-price-for-a-federal-privacy-law/.
———. "A Federal Comprehensive Privacy Law: A Discussion of the Adppa." https://teachprivacy.com/webinar-federal-comprehensive-privacy-law-access/.
The Sound of Economics. Podcast audio. Why is China Cracking Down on Big Tech? https://audioboom.com/posts/7976991-why-is-china-cracking-down-on-big-tech.
Strategic Partnership Agreement between the European Union and Its Member States, of the One Part, and Japan, of the Other Part. 2019.

Stupp, Catherine. "Commission Replaces Safe Harbour with Rebranded 'Privacy Shield'." *Euractiv*, February 3, 2016. https://www.euractiv.com/section/digital/news/commission-replaces-safe-harbour-with-rebranded-privacy-shield/.
Sweet, Alec Stone, Wayne Sandholtz, and Niel Fligstein. *The Institutionalization of Europe.* Oxford: Oxford University Press, 2001.
Swire, Peter. *Us Surveillance Law, Safe Harbor, and Reforms since 2013.".* Future of Privacy Forum (2015). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709619.
Tan, Yeling. *Disaggregating China, Inc.*: Cornell University Press, 2022.
Tanaka, Hiroyuki, Naoto Obayashi, and Noboru Kitayama. "Analysis of Cabinet of Japan's Approved Bill to Amend Appi." (March 18, 2021). https://iapp.org/news/a/analysis-of-japans-approved-bill-to-amend-the-appi/.
Terpan, Fabien. "Soft Law in the European Union Ù the Changing Nature of Eu Law." [In English]. Article. *European Law Journal* 21, no. 1 (01/01 / 2015): 68-96.
Thelen, Kathleen. "How Institutions Evolve: Insights from Comparative Historical Analysis." In *Comparative Historical Analysis in the Social Sciences*, edited by Dietrich Rueschemeyer and James Mahoney. Cambridge Studies in Comparative Politics, 208-40. Cambridge: Cambridge University Press, 2003.
Thomas, Beryl. "What Germany's New Cyber Security Law Means for Huawei, Europe, and Nato." (02/05/2021 2021). https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/.
Tooze, Adam. "China under Pressure, a Debate." *Financial Times* (London), March 24, 2022.
"Top 10 Cloud Providers in India." Back4App, accessed October 12, 2021, https://blog.back4app.com/cloud-computing-providers-in-india/.
Torres, Carla, ed. *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of Us-China Rivalry-European Council on Foreign Relations* ECFR, 2020.
Tsuruoka, Michito. "Abe Shinzo's Legacy in Japan-Europe Relations." *The Diplomat*, September 14, 2020. https://thediplomat.com/2020/09/shinzo-abes-legacy-in-japan-europe-relations/.
"U.S.-E.U. Trade and Technology Council (Ttc)." Office of the United States Trade Representative, accessed June 4, 2022, https://ustr.gov/useuttc.
U.S. Private-Sector Privacy (Participant Guide). Portsmouth, NH: International Association of Privacy Professionals, 2021.
UNCTAD. *Digital Economy Report 2021: Cross Border Data Flows and Development.* United Nations (Geneva: 2021).
"What Are Human Rights?", accessed December 12, 2022, https://www.unicef.org/child-rights-convention/what-are-human-rights.
"United States and European Commission Announce Trans-Atlantic Data Privacy Framework." news release., March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.
USA Freedom Act. 2015.
van Creveld, Martin. *The Rise and Decline of the State.* Cambridge: Cambridge University Press, 1999.
van der Made, Jan. "Senegal to Move All Government Data to Huawei-Run Data Center." (June 25, 2021). https://www.rfi.fr/en/africa/20210625-senegal-to-move-all-government-data-to-huawei-run-data-center-china-africa-macky-sall-information-technology.
Vogel, David. ""Private Regulation of Global Conduct"." In *The Politics of Global Regulation*, edited by Walter Mattli and Ngaire Woods. Princeton: Princeton University Press, 2009.
Vogel, Ezra. *Deng Xiaoping and the Transformation of China.* Cambridge: Belknap Press, Harvard University, 2011.

Vogel, Steven Kent. "Freer Markets, More Rules : Regulatory Reform in Advanced Industrial Countries." Ithaca :: Cornell University Press, 1996.
Voigt, Paul Von dem Bussche Axel. "The Eu General Data Protection Regulation (Gdpr) : A Practical Guide." [In English]. (2017). https://doi.org/10.1007/978-3-319-57959-7.
Voss, W. Gregory. "Cross-Border Data Flows, the Gdpr, and Data Governance." Article. *Washington International Law Journal* 29, no. 3 (2020): 485-531.
Waldman, Ari Ezra. *Privacy as Trust: Information Privacy in an Information Age.* Cambridge: Cambridge University Press, 2018.
Walters, Robert, Leon Trakman, and Bruno Zeller. *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches.* Springer, 2019.
Wang, Flora Y. "Cooperative Data Privacy: The Japanese Model of Data Privacy and the Eu-Japan Gdpr Adequacy Agreement." Article. *Harvard Journal of Law & Technology* 33, no. 2 (Spring2020 2020): 661-91.
Warren, S.D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* IV (December 15, 1890). https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.
Weber, Max. *From Max Weber: Essays in Sociology.* New York: Oxford Press, 1946.
Wessels, Ante, "Broken Data Protection in Eu Trade Agreements." *Foundation for Free Information Infrastructure*, https://ffii.org/broken-data-protection-in-eu-trade-agreements/.
West, Ping, "Timeline: China's Tech Crackdown 2021," Ping West ed. *China Tech Last Week*, August 31, 2021, 2021, https://pingwest.substack.com/p/timeline-chinas-tech-crackdown-2021?s=r.
"What Are the Gdpr Fines?" GDPR.EU, accessed September 25, 2021, https://gdpr.eu/fines/.
"What Is Big Data?" Amazon Web Services, accessed March 3, 2022, https://aws.amazon.com/big-data/what-is-big-data/.
"What Is General Purpose Technology?". In *Handbook of Research on ICTs and Management Systems for Improving Efficiency in Healthcare and Social Care,* edited by Maria Manuela Cruz-Cunha, Patricia Gonçalves and Isabel Maria MirandaIGI Global, 2013.
Wolf, Christopher. " Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border Eu-U.S. Data Transfers." *Washington University Journal of Law and Policy* 43, no. 1 (2014): 227-57. https://openscholarship.wustl.edu/law_journal_law_policy/vol43/iss1/13.
Wu, Emily. *Sovereignty and Data Localization.* Harvard University Belfer Center for Science and International Affairs (Cambridge: 2020).
Wu, Guoguang, "Continuous Purges: Xi's Control of the Public Security Apparatus and the Changing Dynamics of Ccp Elite Politics," Minxin Pei ed. *China Leadership Monitor*, December 1, 2020, https://www.prcleader.org/wu.
Xanthoulis, Napoleon. *Negotiating the Eu Data Protection Reform: Reflections on the Household Exemption.* Vol. 441, 2013. doi:10.1007/978-3-319-11710-2_13.
Yakovleva, Svetlana. "Should Fundamental Rights to Privacy and Data Protection Be a Part of the Eu's International Trade 'Deals'?". *World Trade Review* 17, no. 3 (2018): 477-508.
Yallen, Jordan. "Untangling the Privacy Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation." Article. *Loyola of Los Angeles Law Review* 53, no. 4 (2020): 787-825.
Yang, Dali. "China's Illiberal Regulatory State in Comparative Perspective." *Chinese Political Science Review* 2 (2017): 114-33. https://doi.org/10.1007/s41111-017-0059-x.
Ye, Zhusheng. "China's Transitive Legal System in the Reform Era: Between Rule "by" Law and Rule "of" Law."Ph.D., The Chinese University of Hong Kong (Hong Kong), 2014. https://www.proquest.com/dissertations-theses/chinas-transitive-legal-system-reform-era-between/docview/1674839768/se-2?accountid=11752 (3691981).

Yoshimatsu, Hidetaka. "The Eu-Japan Free Trade Agreement in Evolving Global Trade Politics." *Asia Europe Journal* 18, no. 4 (2020): 429-43.

Yuko, Suda. "Japan's Personal Information Protection Policy under Pressure: The Japan-Eu Data Transfer Dialogue and Beyond." Article. *Asian Survey* 60, no. 3 (2020): 510-33. https://doi.org/10.1525/AS.2020.60.3.510.

"How Billionaire Jack Ma Fell to Earth and Took Ant's Mega Ipo with Him." Reuters, Updated November 5, 2020, https://www.reuters.com/article/ant-group-ipo-suspension-regulators/how-billionaire-jack-ma-fell-to-earth-and-took-ants-mega-ipo-with-him-idUSKBN27L2GX.